# Securing a Large Project with Private Cloud Computing

FedCASIC 2011

Taylor Cooper, Westat

March 23, 2011

# Introduction

- Taylor Cooper, Westat

Senior Systems Staff Member at Westat responsible for Technology Planning & Evaluation and participating on Corporate Technology Committees

Involved in several large scale, complex survey research projects conducted for Federal clients.

# Securing a Large Project with Private Cloud Computing

- Cloud Computing – Why we want it
- Cloud Computing Security Challenges
- Addressing Security via Private Cloud
- A Real World Implementation Example
- Lessons Learned and Conclusions

# Cloud Computing – What is It?

- Pool of resources typically accessible via an internet connection and providing one of more of the following:

  Software as a Service (SaaS) – Software applications delivered over the internet.

  Platform as a Service (PaaS) – Development environments, Collaboration site, etc. provisioned as an integrated solution and delivered over the web.

  Infrastructure as a Service (IaaS) – Computer infrastructure, typically a platform virtualization environment as a service.

# Cloud Computing – Why We Want It

- It’s Shiny and New! – Clients and managers like to brag.
- It’s Flexible! – Dynamically ramp resources up and down to meet demand
- It’s Cost Effective! – Only pay for services you need; Don’t get left holding the bag on old hardware in 3 years.
- It’s Manageable! – Get away from managing configurations and applications on large numbers of end-user laptops and workstations.

# Cloud Computing – Why We Want It

- It’s Available! – Have an internet connection?  You have access to your data and applications!
- It’s Faster! – Applications, Databases and Servers are all running on networks and hardware at the datacenter.  The speed of the end user equipment and connection is much less important.
- It’s Independent! – Underlying hardware and end-user machines are independent of the virtualized servers and applications.  Hardware can be upgraded, and lost field equipment can be replaced much more easily.

# Cloud Computing Security Challenges

- Is My Data Safe? – Organizational policies for storage and handling of PII require direct oversight and control.
- Where is that Data Exactly? – Client agency's interpretation of regulations affect the physical location of confidential data (e.g., CIPSEA).
- Whose Cloud Is This? – Perceived loss of control and ability to respond to emergency situations. Inherited/Assumed Risks if Cloud Supplier's SLAs are not met.

# Cloud Computing Security Challenges

- Just How Big is this Cloud? – Difficulty meeting physical control audit review requirements if operations exist in multiple locations.
- Who's Going to Fix This? – Security monitoring & vulnerability assessments must be continuous and Security Audit Remediation may require changes by the cloud provider
- The Sky is Falling! – Ability to 'pull the plug' in an emergency may be compromised or delayed.

# Addressing Security via Private Cloud

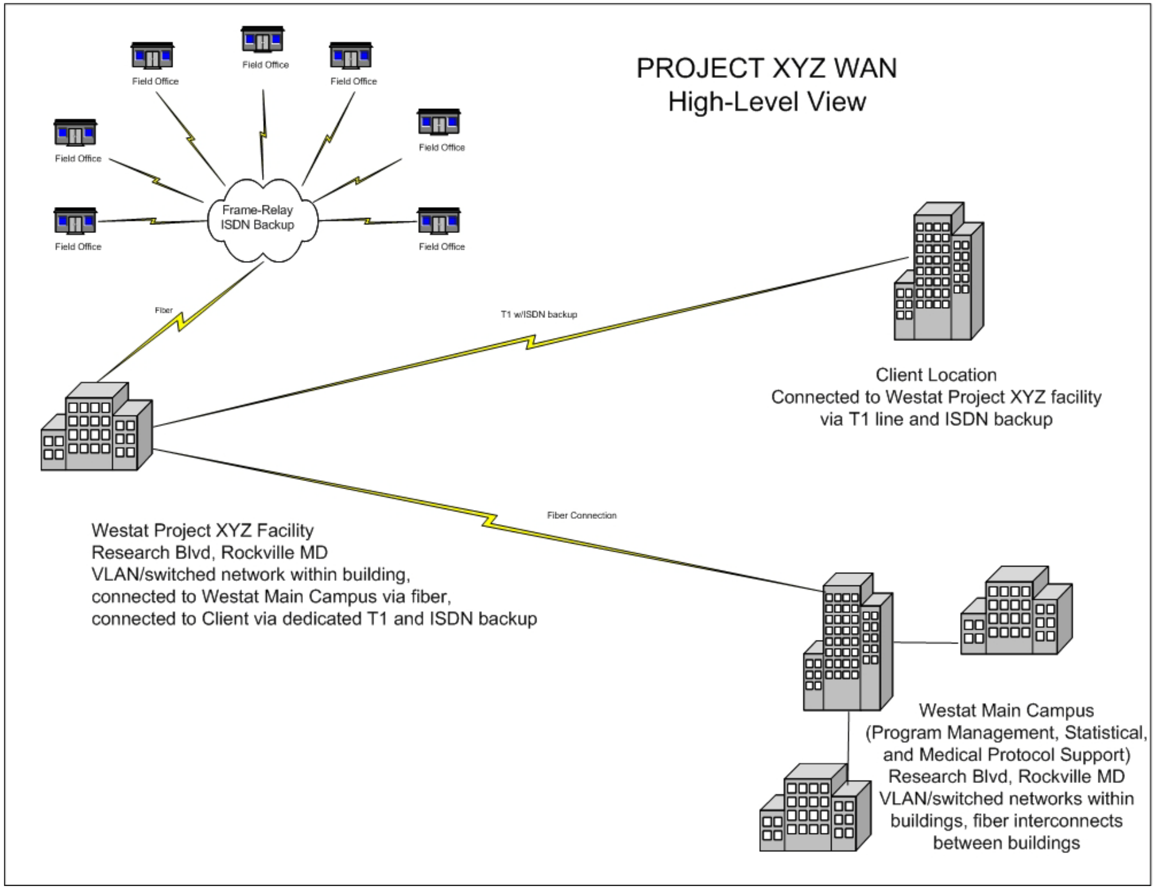
- Ability to satisfy FISMA-moderate certification and FIPS 800-53 audit requirements including physical site security controls.
- Ensure data in motion and data at rest meet FIPS 140-2 encryption requirements.
- Ability to demonstrate failover and recovery of all system functions within desired timeframes.
- Defined system boundaries to support continuous monitoring and vulnerability assessments.

# Addressing Security via Private Cloud

- Private cloud approach
- Technological benefits of cloud computing
- Defined hardware resources and physical network boundaries
- Ability to manage and reconfigure resources as needed

# A Real World Implementation Example

## Transforming a Distributed Legacy Infrastructure



PROJECT XYZ WAN
High-Level View

Client Location
Connected to Westat Project XYZ facility
via T1 line and ISDN backup

Westat Project XYZ Facility
Research Blvd, Rockville MD
VLAN/switched network within building,
connected to Westat Main Campus via fiber,
connected to Client via dedicated T1 and ISDN backup

Westat Main Campus
(Program Management, Statistical,
and Medical Protocol Support)
Research Blvd, Rockville MD
VLAN/switched networks within
buildings, fiber interconnects
between buildings

# A Real World Implementation Example

## Transforming a Distributed Legacy Infrastructure

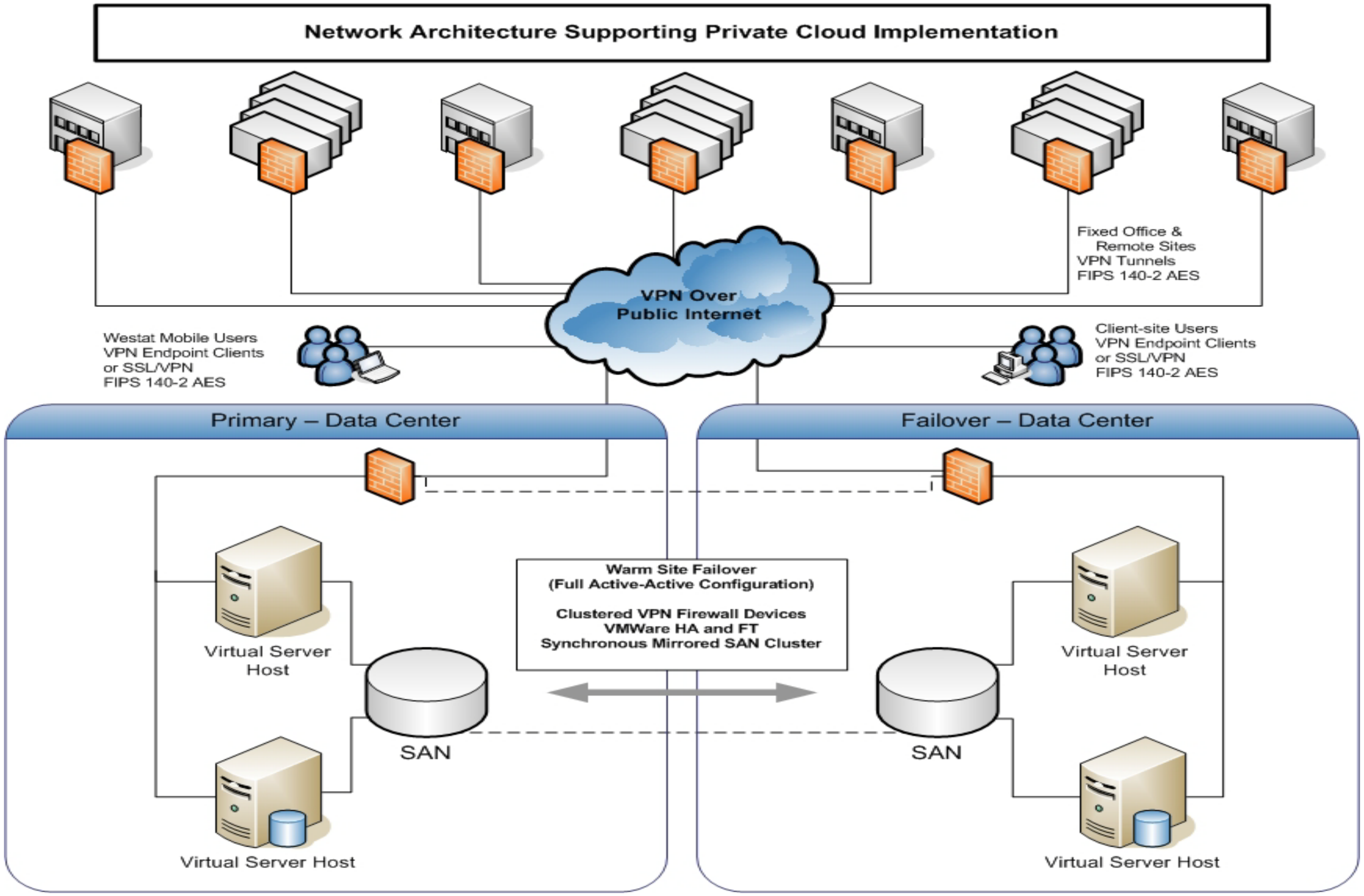
- Database Servers operating at remote field locations and replicating data
- Applications and runtime environments installed on every workstation (100+ machines)
- Fixed-bandwidth, provisioned private WAN links incurring cost based on data usage

# A Real World Implementation Example

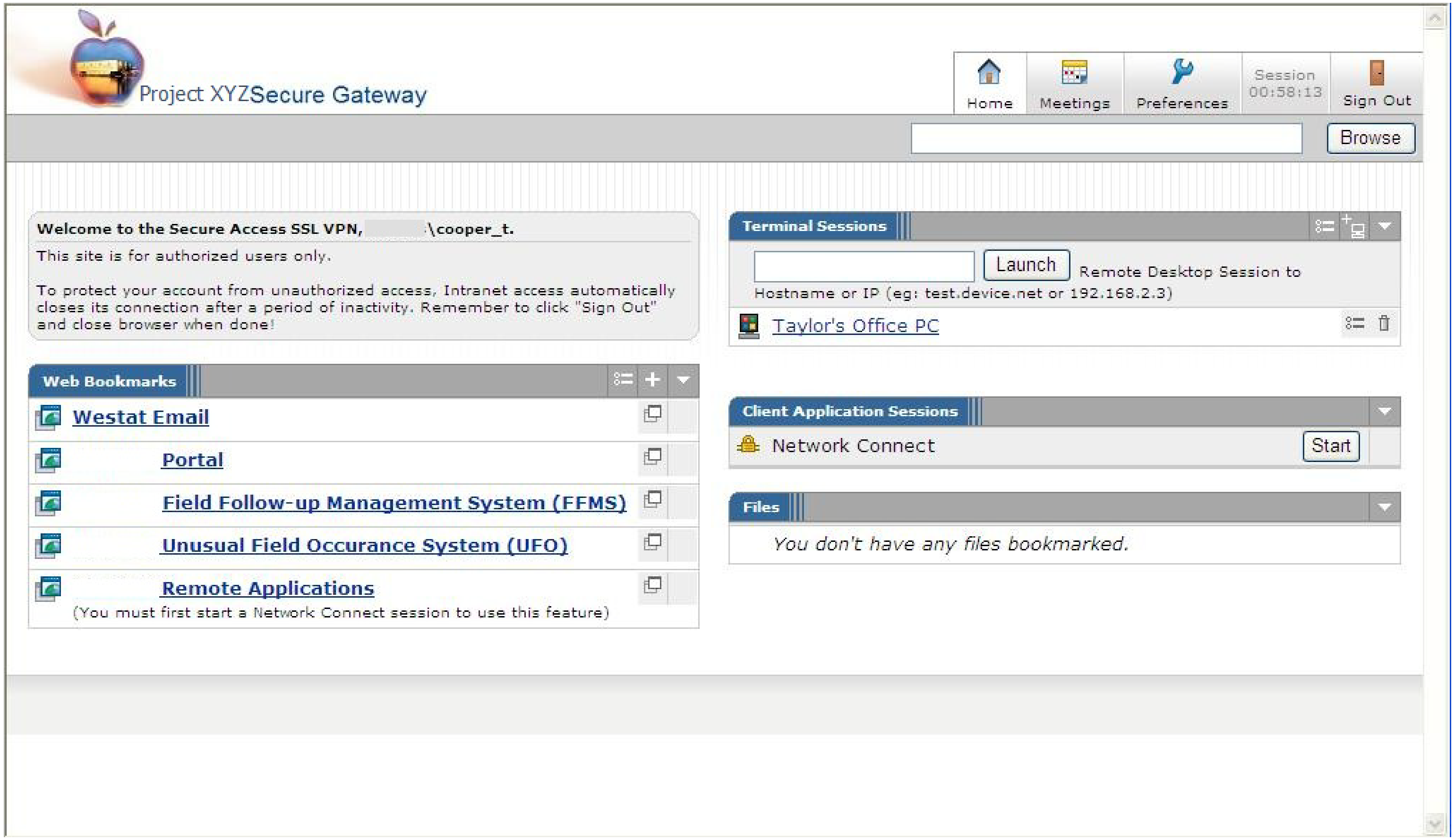
## Transforming a Distributed Legacy Infrastructure

- “Mission Critical” components (i.e., production database) recovered to alternate site within 8 hours. Remaining systems prioritized and recovered in 48+ hours.
- Training limited to standalone applications and databases, or physically on-site
- Extended 48-hour maintenance windows to accommodate database changes across the distributed system, hardware maintenance, patching, security scanning, etc.

# A Real World Implementation Example
# Infrastructure



# A Real World Implementation Example
# “PaaS – Platform as a Service”



Project XYZSecure Gateway

Welcome to the Secure Access SSL VPN, \cooper_t.

This site is for authorized users only.

To protect your account from unauthorized access, Intranet access automatically closes its connection after a period of inactivity. Remember to click "Sign Out" and close browser when done!

**Web Bookmarks**

- Westat Email
- Portal
- Field Follow-up Management System (FFMS)
- Unusual Field Occurance System (UFO)
- Remote Applications
  (You must first start a Network Connect session to use this feature)

**Terminal Sessions**

Launch Remote Desktop Session to Hostname or IP (eg: test.device.net or 192.168.2.3)

- Taylor's Office PC

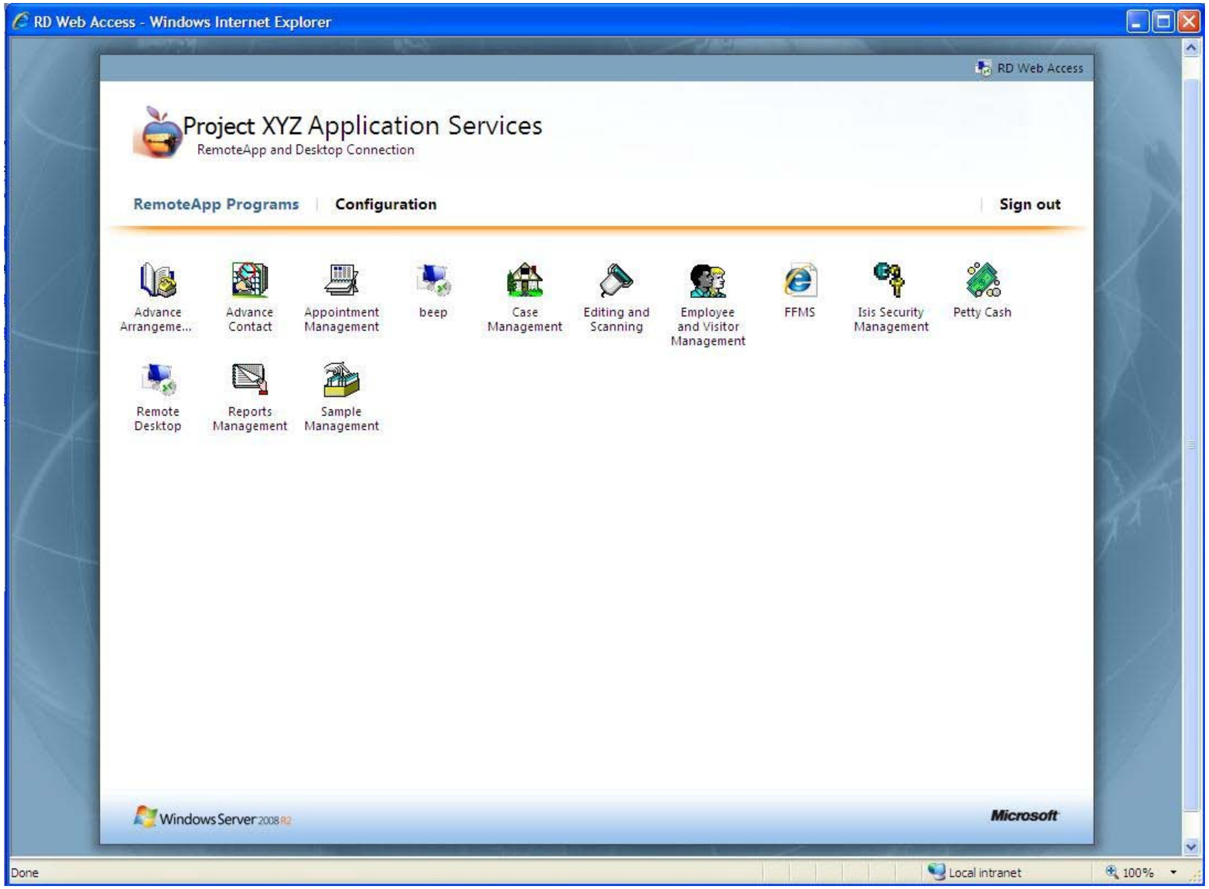
**Client Application Sessions**

- Network Connect — Start

**Files**

*You don't have any files bookmarked.*

# A Real World Implementation Example
# “SaaS – Software as a Service”



# A Real World Implementation Example
# Private Cloud – Security Features

- Independent, non-Trusted Active Directory Domain
- User authentication against Active Directory
- Routine Scans using Tenable Nessus
- Log Monitoring and Analysis using Splunk
- Uptime monitoring and Accessibility using RGE IPSentry

# A Real World Implementation Example
# Private Cloud – Security Features

- Database dumps “data at rest” encrypted using RedGate SQL Backup
- Remote Sites – site-to-site VPN using AES encryption
- External Users – SSLVPN using AES encryption
- Cloud operates on its own IP Network Segments
- Border Gateway running Intrusion Detection and Prevention (IDP), Web Filtering, Access Controls

# A Real World Implementation Example – Benefits Realized

- Single, unified model for site failover and disaster recovery.  Full system failover capability.
- ~80% reduction in datacenter footprint.  Reduced from 6 racks of equipment spread across Westat, client and field locations down to 1/2 rack at two datacenters.
- Centralized management and administration of servers and applications, plus VPN over internet resulted in approximately 15% annual IT cost reduction.

# A Real World Implementation Example – Benefits Realized

- Security audit can focus on an identifiable pool of physical host servers and virtual servers running on those hosts.

- System availability and reliability is operating at over 99%.  in 1 year of continuous operation, we experienced a 2 hour unplanned database outage, and scheduled maintenance downtime has been reduced significantly.  Previously, maintenance windows were six per year and ran for 48 hours (~280 hrs/yr).  This has been reduced to six 4-8 hour maintenance windows. (~36 hrs/yr).

# A Real World Implementation Example – Benefits Realized

- Greater flexibility. Allows training staff against cloud-based training databases and applications from hotels, conference centers or any site supporting an internet connection.

- By virtualizing applications and running them inside the cloud, all data processing, storage, and backup is secured and managed within the datacenter. Loss or failure of end-user equipment has minimal impact.

# A Real World Implementation Example – Cost Considerations

- Requires an equipment investment.  Break-even point between legacy fortress configuration and private cloud was at the 20-25 server mark.  In our example, we converted/consolidated 27 physical servers into 22 virtual servers.
- Full system failover capability = twice the resources.
- Requires staff with qualification in sought after technologies -- SAN, Virtualization, Security, WAN/VPN.

# Lessons Learned and Conclusions

- Just because you can provision and deploy virtual servers quickly doesn't mean you should!  You still have to manage resource pools and you still have to license servers and software.
- Plan ahead and don't over allocate resources.  It's easier to grow virtual server's disks and add cpu/memory resources than it is to try and reclaim over allocated resources.

# Lessons Learned and Conclusions

- Consider enterprise and datacenter licensing models.  If you are running multiple environments (e.g., development, demo/train, acceptance, production) in your virtual server space on limited number of physical host hardware you may be better off with an enterprise version that does not require you to license individual virtual servers.
- While any machine with a web browser and a user with credentials can access the cloud.  It's a good idea to implement some sort of remote machine host checker to verify active anti-virus, patch levels, identification tokens, etc.

# Lessons Learned and Conclusions

- Public Cloud solutions claim to be secure and operate to FISMA moderate standards, but clients are still hesitant to put sensitive or mission critical data ‘out there’.
- Private Cloud results in most of the benefits promised by cloud computing but incurs infrastructure costs.
- Private Cloud presents physical boundaries that are more easily secured and audited versus Public Cloud implementations.

# Securing a Large Project with Private Cloud Computing

Contact Information:

Taylor Cooper, Westat

TaylorCooper@Westat.com

301.610.4902