WSDOT: Sharing data with trusted partners

A plan for flexible information sharing with WSDOT affiliates

Final Report

29 June 2007

Contents

Objective

- To help the WSDOT determine how to provide trusted business partners with flexible, secure access to WSDOT systems and data
- Access method should meet current and anticipated data sharing requirements

Acronyms/Terms

as used in this report

DMZ (literally, demilitarized zone): A separate sub-network for resources to be shared with trusted and semi-trusted networks and secured from the trusted network

FTP (file transfer protocol): Secure or un-secure transfer of data from one computer to another over the Internet

RDP (remote desktop protocol): Multi-channel protocol that enables connections to a computer running Microsoft Terminal Services, which allows remote control of Windows XP, 2003 and Vista.

SSL (secure sockets layer): A software protocol for secure (encrypted) communication between client and server

Sandbox: A duplicate, or replicated, system or database available for access and data manipulation without changing the original system

Semi-Trusted Sandbox: A network which may be contained within a trusted network, but is fire walled from the trusted network so that external connections can be safely terminated in the sandbox

VPN (virtual private network): Technologies that enable secure network access via un-trusted networks by using encryption plus user and data authentication

Situation

- WSDOT needs to share information with a wide array of information consumers including:
  1. The general public
  2. Contractors and vendors
  3. Other government agencies
- This report does not address information sharing with the general public
- Some information that the WSDOT wishes to share with #2 and #3, above, is contained in internal systems which must be protected from un-trusted networks including the Internet and non-WSDOT networks

Requirements

- Trusted business partners need access to WSDOT information resources. Partners include:
  - Washington and Federal government agencies, counties, and cities
  - Consulting firms, contractors, and sub-contractors
- Access requirements vary: Some partners need read/write access to databases, others need files, still others have project specific requirements
- Solution must conform to DIS standards to accommodate impending reconnection to DIS network

Status:
Infrastructure and Architecture

- Current information sharing is *ad hoc*, but includes SSL access to SharePoint (token authenticated), FTP access to an external/DMZ host, e-mail and outward facing Web posting
- Data stewards control access to specific information sources, but not in a uniform way or using specific standards

Status:

Infrastructure and Architecture (cont.)

- Typical perimeter architecture, internal switched networks with routing and segmentation capabilities
- DMZ(s) currently architected to support truly external facing systems: WWW, FTP, etc.
- Additional internal segmentation could support access to a semi-trusted sandbox where WSDOT terminates trusted partners connections

Observations

- Current security and integrity of information flows depend on smart people always making the right decisions in the absence of uniform procedures or guidelines
- Neither data nor partners are formally classified in terms of sensitivity or access
- No clear policy that outlines the decision authority for sharing information and unclear ultimate authority for sharing and access
  - Not all shared information appears to have a Data Steward
  - Data Steward process isn't published nor is it part of a written policy
  - "Data Steward" seems to have more than one definition as described in interviews

Observations (cont.)

- Many excellent security polices are in place; however, guidelines and procedures to address specific cases seem to be lacking
- Per interviews, personnel seem to interpret current policies slightly differently
- Projects like the Alaska Way Viaduct project present new complications as consultants need read/write access to live WSDOT databases

Solutions to three needs

- We considered three separate requirements:
  - Read and Read/Write access to databases
  - File transfer, both inbound and outbound
  - Client/Server access to internal systems

Solution: Database access

The current SSL VPN project is what we would have recommended for the access component.

Other data access methods considered included:

- Direct native access through VPN, database or client/server tools, and
- Remote terminal access, directly or through RDP

Solution: Read-only database

- Read-only database access is best accomplished by abstracting the SQL language using a query construction portal
- Pre-built portals, such as the Codeplex tools, are not flexible enough to meet current, much less future, needs of the WSDOT and are not designed as security products
- A custom built Web portal could accommodate canned reporting as well as on-the-fly SQL generation based on business rules built into the portal

Solution:

Read-only database: SQL construction portals

- A query construction portal would allow for *ad hoc* SQL queries to be constructed, but only using the SQL language constructs the user is allowed by the portal
- Since the wizard-like interface will only yield deterministic queries, the impact to the SQL databases can be minimized
- The same portal can also easily accommodate canned reports

Solution: Read/Write database

- Read/Write database access to critical information systems from outside partners is a high risk access scenario, e.g., Alaskan Way Viaduct project's current requirements for their software development partner
- If this access is required, it should be allowed only to replicated data and synchronized with care to internal databases
- Read/Write database access to non-critical information systems could be allowed to non-replicated databases, given that the recovery costs for non-critical systems is low and recovery can be accomplished quickly
- SSL VPN with partner sandbox connection termination and multi-factor authentication are strongly recommended for this access

Solution:
Replicated sandbox databases

- Advantages:
  - Allows for isolation in cases where data integrity is suspect
  - Provides for greater availability for internal databases in the case of vendor/sandbox security incident
- Disadvantages:
  - Can cause synchronization problems

Solution: Client/Server

- Client/server access to WSDOT systems suffers from the same risks as read/write database access and should follow the same guidelines
- SSL VPN termination into partner sandbox, replicated data – carefully synched back to live WSDOT systems

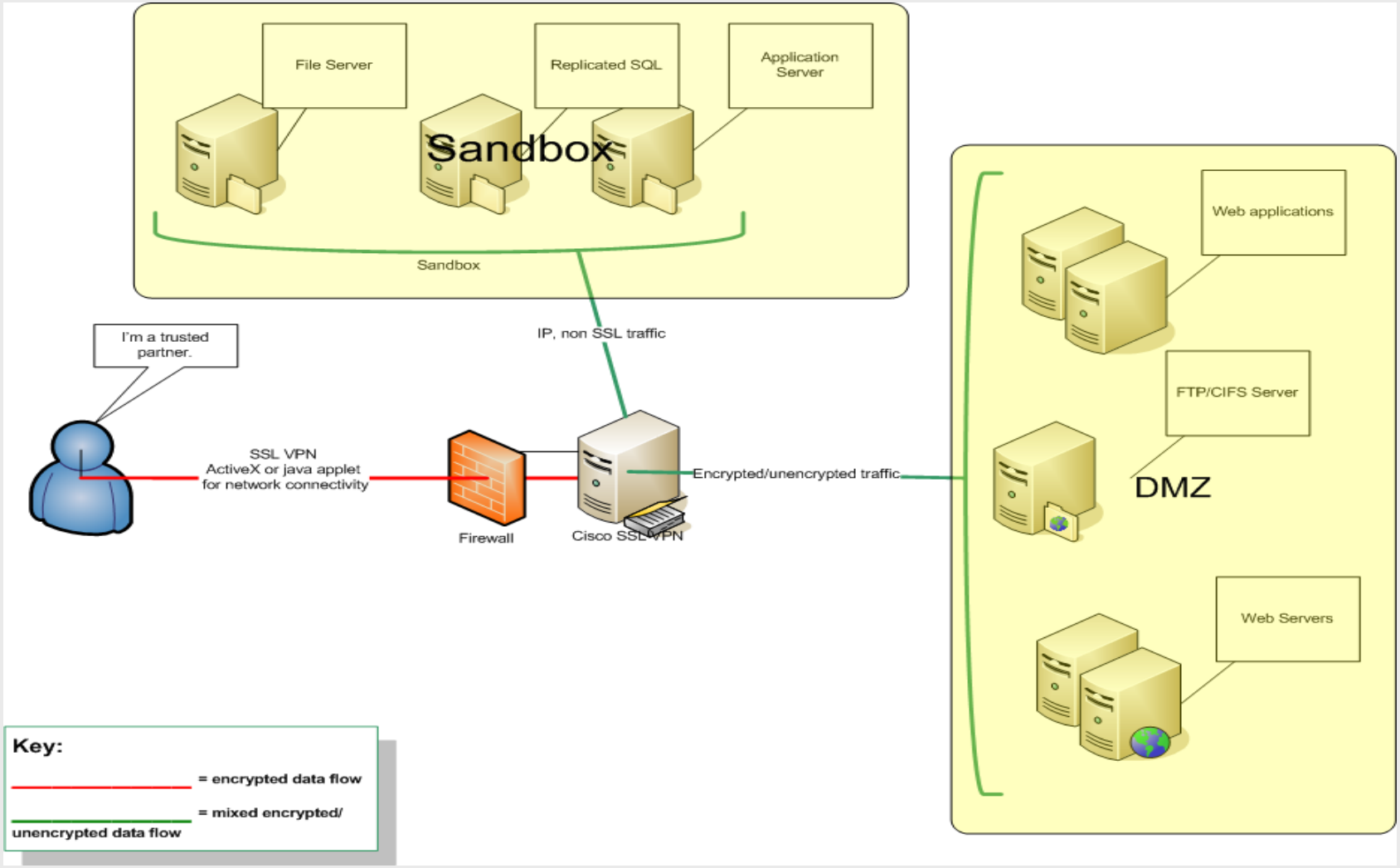
Solution: File transfer

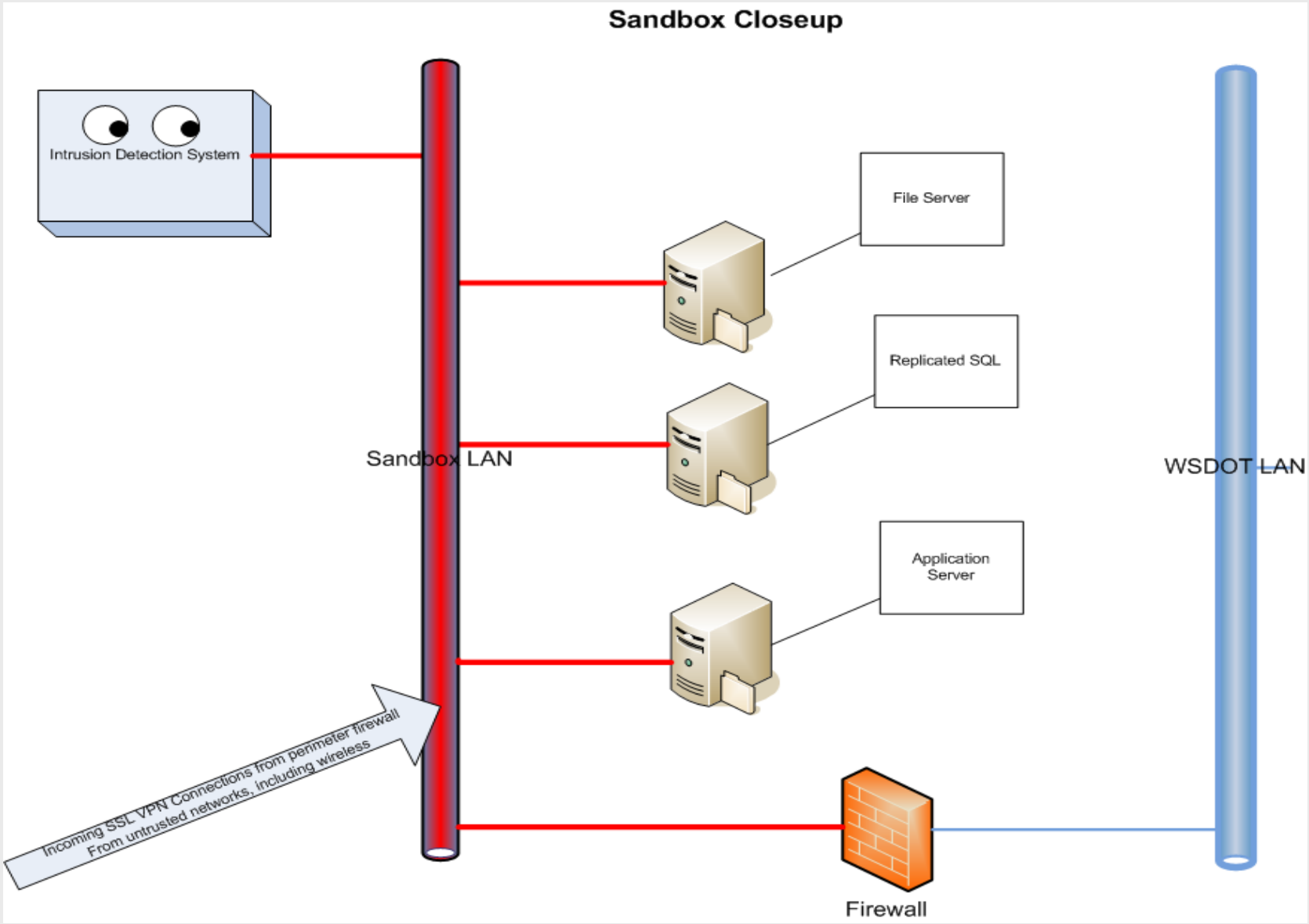
- File transfer is something handled directly by the proposed Cisco SSL VPN, with built-in authentication, authorization, and access controls
- As with other external access, we suggest no direct access to primary data sources, but VPN termination into a partner sandbox with data either automatically or manually replicated to file/FTP servers in the sandbox

Sandbox construction

- Relatively low activity (compared to internal networks) allows for increased vigilance through intrusion detection systems, intrusion prevention systems and virus scanners. All logging and prevention turned up as high as is practical
- Single point of interaction with internal networks allows for strong clear firewall rule base
- Semi-trusted nature allows for termination of partner connections to a network with sensitive information without complicating the perimeter firewall rules to accommodate a semi-trusted DMZ
- Internal placement of the sandbox allows for easier maintenance of the sandbox systems, rather than traversing the perimeter firewall for backup and other maintenance tasks

Proposed solution




Sandbox Closeup
Intrusion Detection System
File Server
Replicated SQL
Application Server
Sandbox LAN
WSDOT LAN
Incoming SSL VPN Connections from perimeter firewall
From untrusted networks, including wireless
Firewall

Estimated costs

- Cisco SSL VPN single point of contact:
  - Internal project underway, no additional cost
- Partner sandbox implementation:
  - 200 hours, internal resources
  - Replicated servers for SQL Server, file transfer hosts, application hosts
    - Estimated hardware and software cost: $120,000
  - SQL query construction portal, WSDOT design and build
    - $150,000 for base functionality

Summary

- The ongoing SSL VPN single point of contact implementation is *exactly* what we would have recommended and a large part of the solution
- The current Citrix/Safeword implementation can be augmented with MobilePass, another offering from Secure Computing, that eliminates hardware tokens in favor of real-time e-mail delivery of onetime use passwords and will co-exist with current installation as an *extension* of the current Safeword solution

Summary (cont.)

- A controlled layer of abstraction for SQL server reports/queries allows the WSDOT complete control over what partners see on an individual basis
- Replicated servers and databases allow for built-in delays and transactional separation for read/write database access
- Sandbox isolation gives the WSDOT a single place to watch with intrusion detection, anomaly detection, and other means

Appendices

- Acknowledgement
- Classifying partners and data
- Policy example
- Employee education
- iSchool team members and contacts

Acknowledgement

The University of Washington Information School team would like to express our sincere appreciation for the time, effort, and patience extended to our team during a project that by its nature required some tough questions and equally tough answers – all compressed into a very short time frame. Without exception, our interactions with the Washington State Department of Transportation team members have been professional, informative, insightful, and even delightful, creating an environment where our analysis became a true product of collaboration between the Information School and the WSDOT.

To each of the WSDOT team members who made this successful collaboration possible, we extend our thanks and our hopes that this project has provided insight into the challenges presented.

Classifying partners and data

- Consider categorizing users by role or employee vs. non-employee
  - E.g., WSDOT employee, employee of other state agency, project partner, member of the public
- Consider classifying data by sensitivity
  - E.g., standard security classifications (sensitive, confidential, classified, top secret, etc.) or other classification system devised in-house
  - Ensure that definitions are widely understood

Policy example

(Policy 900.11, Secure File Transfer)

Current

The policy describes why secure file transfer is important, why the policy is necessary, safeguards that should be in place (e.g., encryption) and who is responsible for assessing the risk, etc.

Suggested

Add guidelines and procedures:

- Include information that tells readers how to encrypt files they need to share, which transfer channels are most secure, which transfer channels should never be used, etc.
- Include reference or link to the related policy on data sharing.

Employee education

Educating employees regarding security and compliance issues can be costly. However, it is worth the investment. Some inexpensive education ideas include:

- Poster campaign describing data classification, partner classification, and other key topics
- E-mail newsletter to all employees. For example, it could be quarterly and describe good/poor practices, highlight employees who have done great things with regards to data security
- Online policy education and testing

iSchool team

Robert M. (Bob) Mason, Ph. D.
Associate Dean for Research for the iSchool
rmmason@u.washington.edu

Barbara Endicott-Popovsky, Ph. D.
Director, Center for Information Assurance and Cybersecurity (CIAC), University of Washington

Michael Simon, lead consultant
Chief Technical Officer, Creation Logic
msimon@creationlogic.com

Robert E. (Bob) Larson
SQL Server/Data Architect & Lecturer, iSchool

Kim McCrea
Student Research Assistant