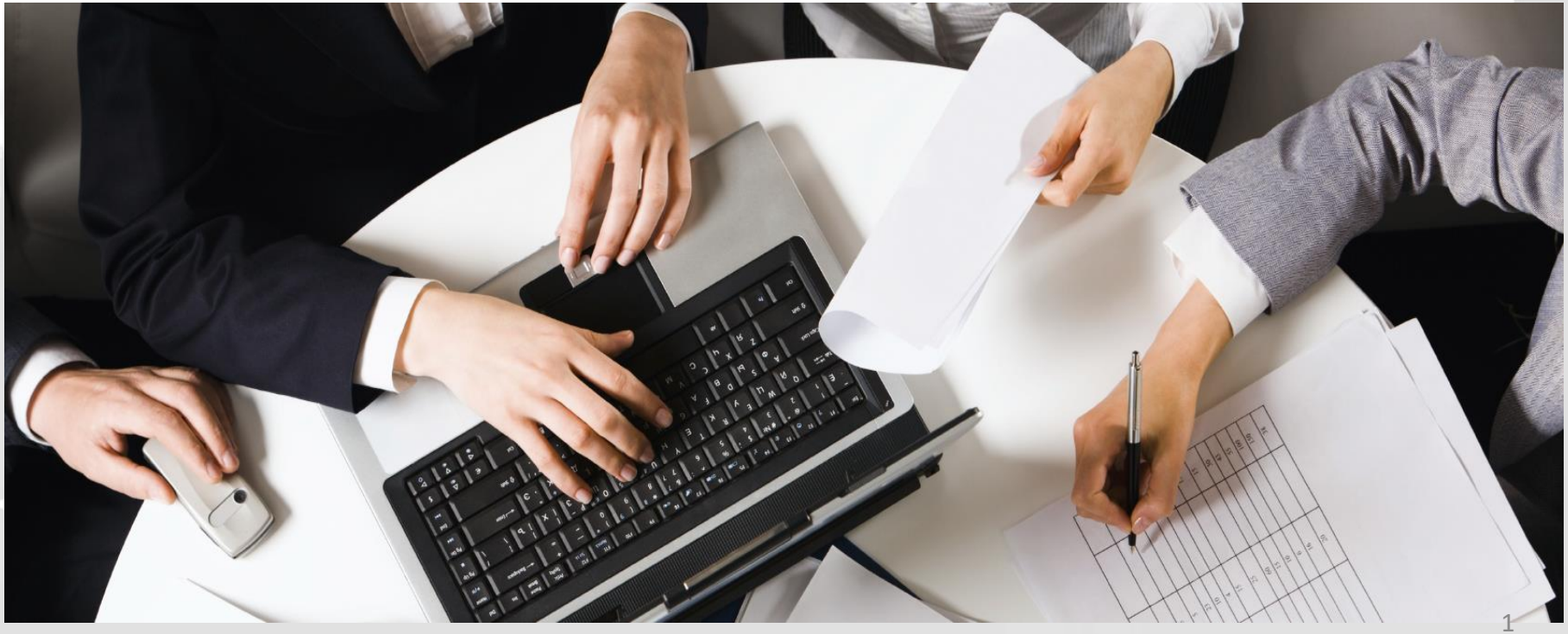
Software Diversified Services

Security Solutions for the Mainframe



Agenda

- Introductions and Company Overview
- Why is FTP so Vulnerable ?
- Options available to Secure FTP
- Live Demo of migrating to SFTP without any JCL changes
- Questions

Introductions

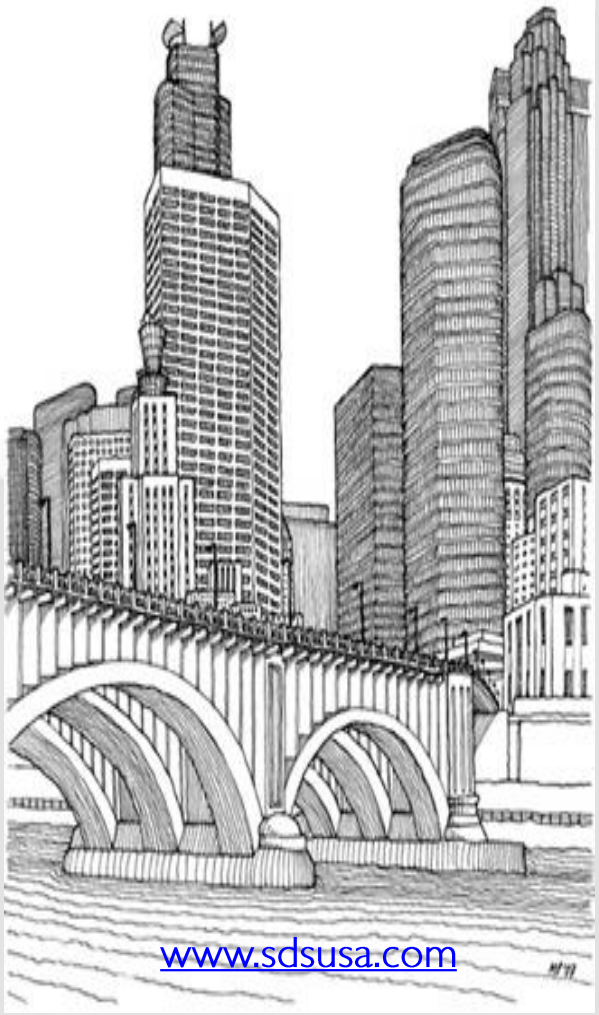
Colin van der Ross

Senior System Engineer

Software Diversified Services
Proudly Serving Enterprise Customers for Over 36 Years

- Financially Rock Solid
- Several Hundred Satisfied Licensed Customers Worldwide
- Over 20 z/OS, z/VSE and z/VM Mainframe Systems and Distributed Products
- World Class Support

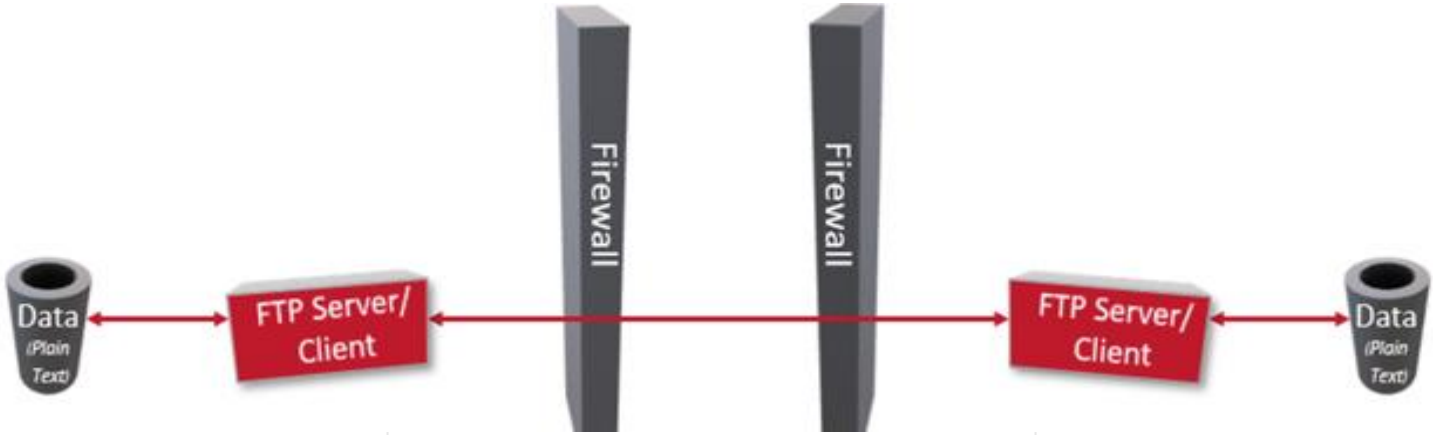
  Full Time Development / Support Staff / USA
- Partner Solutions - Virtel Web Solutions, ConicIT, SSH Tectia for z/OS (Secure FTP)
- VitalSigns SIEM Agent for z/OS
- IronSphere and FIM+



HQ in Minneapolis
1322 81st Ave. NE
Spring Lake Park, MN
55432-2116 USA

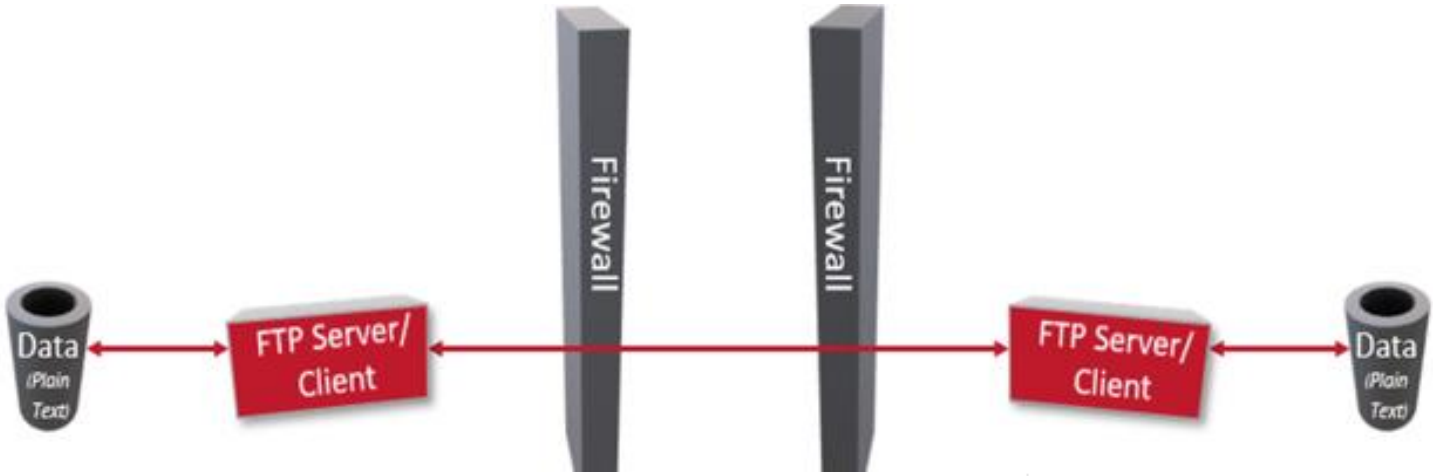
(800) 443-6183,
(763) 571-9000

Why is FTP so Vulnerable



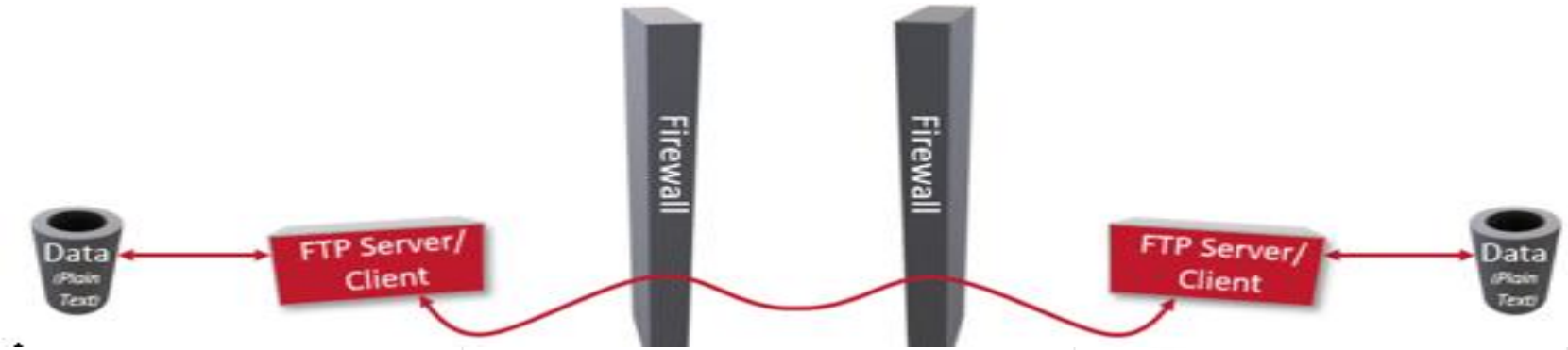
- FTP
- Ubiquitous
  - ✓ Readily available on most platforms. Client side is always ready to go, and the Server requires some configuration and can be available
- Common Knowledge
  - ✓ Been around for such a long. Easy to use. Command Syntax is simple. Almost everyone has used FTP
- Included in the OS

Why is FTP so Vulnerable



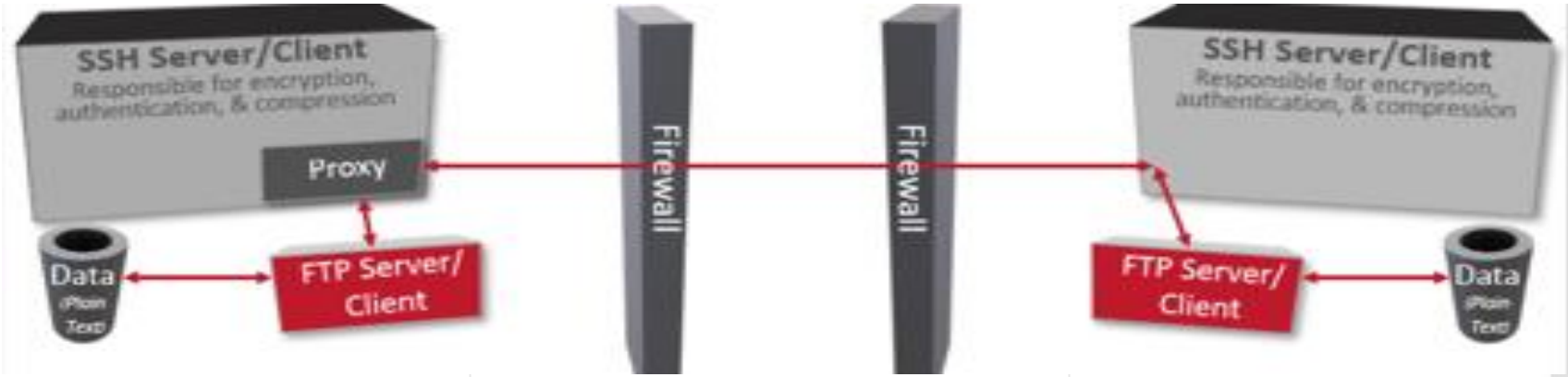
- Very Little Security
  - × FTP is a CLEAR text protocol . That means any eavesdropper can see the User IDs , password and data with the appropriate tools
- × Not Firewall Friendly
  - × Strange" protocol – designed around having 2 connections,. One for commands and the second one for the data transfers
  - × No Native compression
  - × Lacks Integrity Validation

Options available to secure FTP



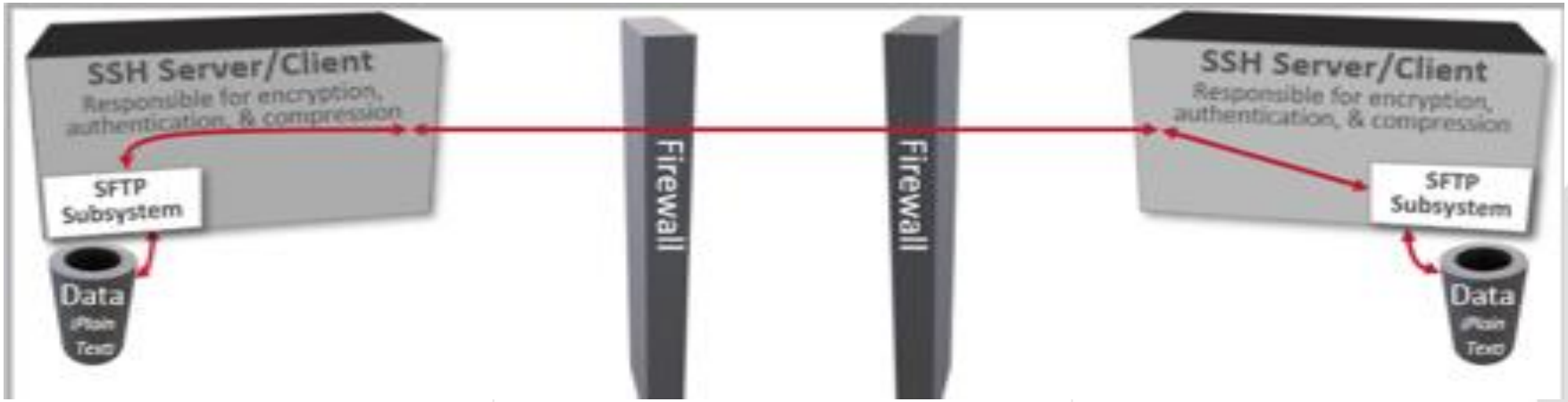
- FTPS - FTP over SSL
  - ✓ Similar to FTP
  - ✓ Included in the Base OS
  - ✓ Supports x.509 certificates
  - × Not Firewall Friendly
  - × Can't assume its available on the other end

Options available to secure FTP



- FTP over SSH Tunnel
  - ✓ Same FTP familiarity
  - ✓ Firewall Friendly
  - ✓ Compression of data
  - ✓ Good data checksums
  - × More parts need to be choreographed
  - × Requires SSH and FTP on both ends

Options available to secure FTP

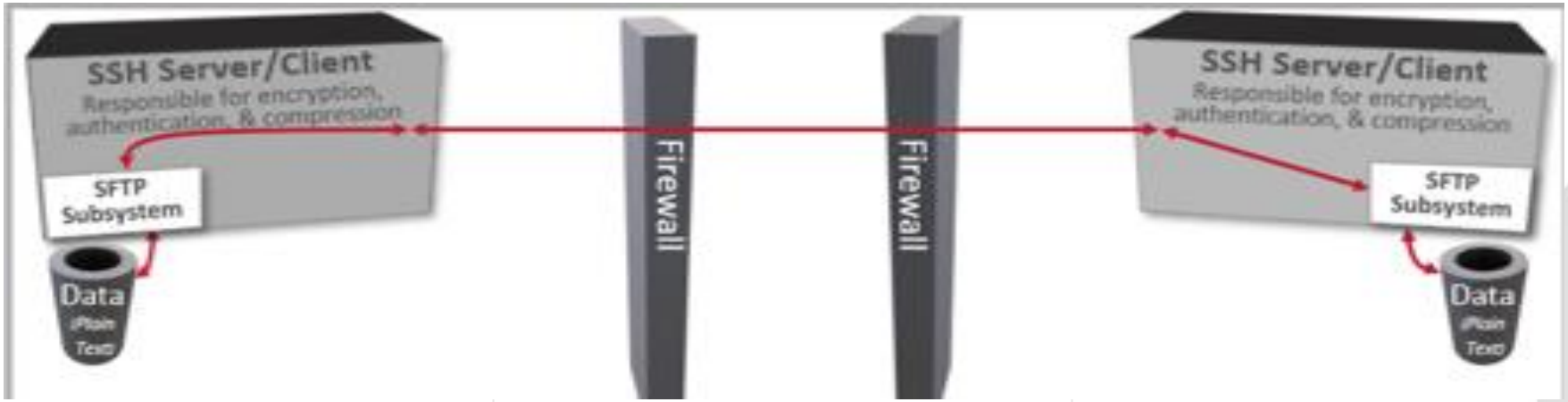


- Secure FTP (SFTP)
  - ✓ Satisfies the SFTP requirement
  - ✓ Point to Point Encryption
  - ✓ Compression / Integrity built in
  - × May not be part of your operating system
  - × May not be familiar to users
  - × Only protects the data in transit

Options available to secure FTP

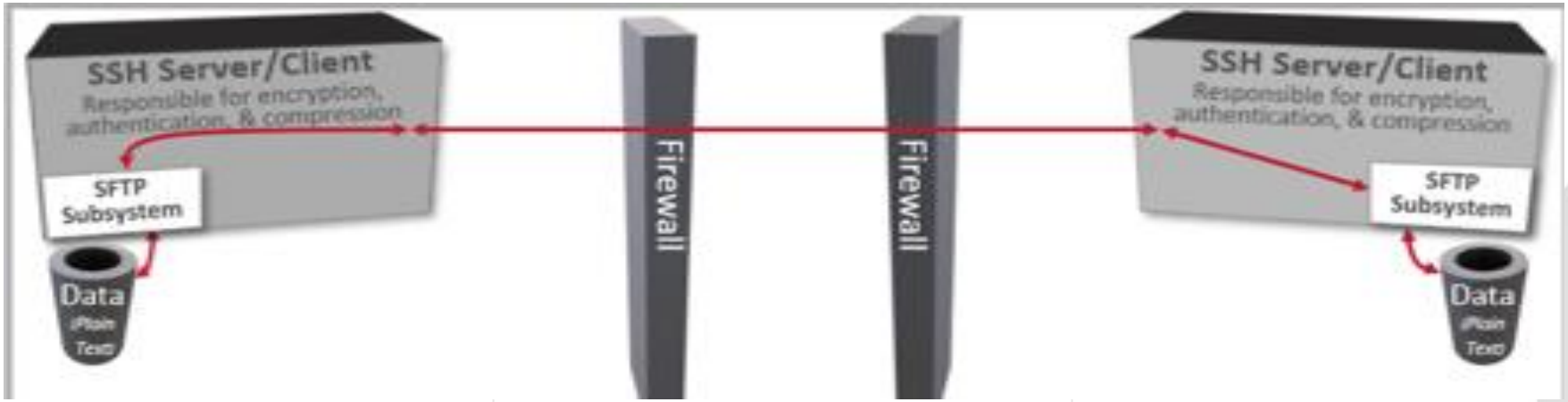
- PGP (Pretty Good Privacy)
  - ✓ Secures data at Rest not in motion
  - ✓ Full control of sensitive data
  - ✓ Compression and integrity built in
  - ✓ Not Just for transfers
  - × Requires staging

Options available to secure FTP



- <u>FTP to SFTP Conversion</u>
  - ✓ Satisfies the SFTP requirement
  - ✓ Can still use the FTP client on the z/OS side
  - × Not a perfect match

Options available to secure FTP



FTP to SFTP Conversion – Demonstration

- Tasks already completed
  - VFTP and SSH installed
  - Uploaded the remote servers public key
  - Configured the SSH Proxy to convert FTP to SFTP
  - Configured VFTP to route batch job ZFTPJOB to the SSH Proxy

FTP to SFTP Takeaways

- Surprising to see how many customers still use FTP
- Many options to consider
- Not a "one size" fits all
- Could be one solution of a combination of solutions presented here this evening
- What is the end goal ?

Questions

Agenda

- [ ] What is a SIEM?
- [ ] Demo of SMF events being sent to QRadar / Splunk
- [ ] Demo of Granular Filtering
- [ ] Suggested SMF 80- Events to monitor (as per SDS customers input)
- [ ] Questions

What is SIEM ? – Security Information & Event Management

- Security Management provides a holistic view of an organization's information technology security
- SIEM combines SIM (Security Information Management) and SEM (Security Event Management) functions into ONE Security Management System

SIEM – Security Information & Event Management

Security Information & Event Management System	
Security Event Management (SEM)	Security Information Management (SIM)
Provides - ▶ Event Management ▶ Real Time Threat Analysis ▶ Incident Detection & Response ▶ Basic ticketing capabilities ▶ Security operations	Provides - ▶ Centralized log collections ▶ Long term log collection ▶ Log search and reporting

Why SIEM?

Security Requirement

- SIEM is the core of a defense in-depth strategy
- Attackers leave behind a trace – Logs
- Security Events provide insight into
  - When the event occurred
  - Why it happened
  - What happened

Why integrate z/OS into SIEM ?

- Compliance Requirement
  - PCI, SOX, HIPAA,GLBA, etc
- Mainframe contains Sensitive data
  - Large corporations have 70% of data on Mainframes
- z/OS is not invulnerable
- You already have a SIEM, why not use it for your mainframes ?

SIEM – One view of your entire Enterprise

- A Enterprise SIEM collects / aggregates logs from heterogeneous sources
  - Databases
  - Routers
  - Switches
  - Other SYSLOG devices
- All in ONE central location

SIEM – One view of your entire Enterprise

- Makes searching easy
  - Exact Time
  - Corresponding Security Event
  - Who
  - When
  - Location

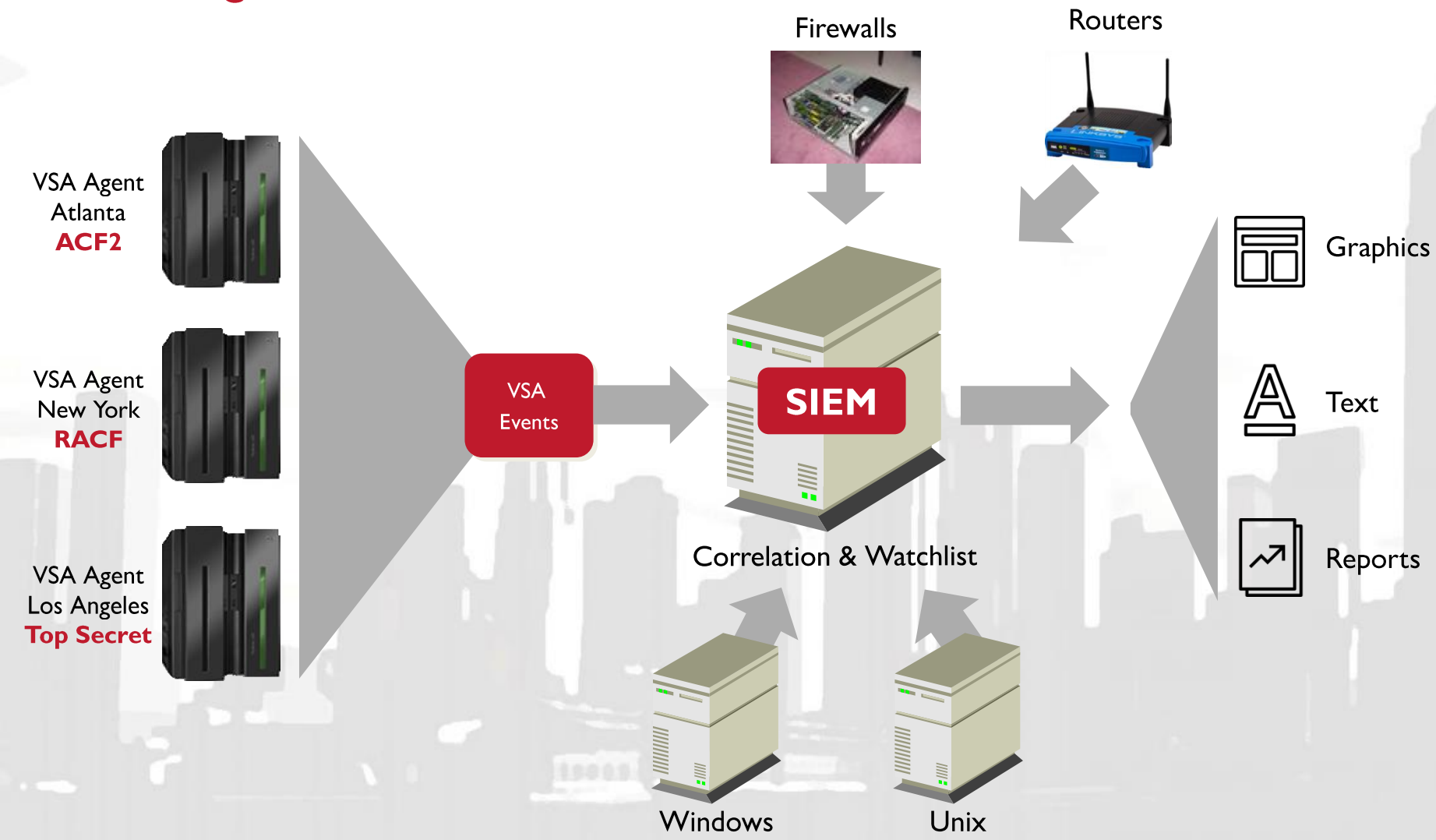
SIEM – One view of your entire Enterprise

- Configure Rules
- Kick off scripts
  - Based on thresholds
  - Conditions
  - Violations
  - Anomalies

SIEM – One view of your entire Enterprise

- Historical Data
- Compliance Requirements
- Logs are tampered proof

VSA Integration



SMF Types Monitored by VSA

- Record Type 14 (0E) -- INPUT or RDBACK Data Set Activity
- Record Type 15 (0F) -- OUTPUT, UPDAT, INOUT, or OUTIN Data Set
- Record Type 17 (11) -- Scratch (delete) of Data Sets
- Record Type 18 (12) -- Rename of Data Sets
- Record Type 30 (1E) -- JOB/STEP TERMINATION (BATCH, TSO, STARTED TASK)
  - TYPE30_I: Job Initiation
  - TYPE30_4: Step Termination
  - TYPE30_5: Job or Session Termination
  - TYPE30_6: System Address Space
  - TYPE30_D: DD Segment Detail
  - TYPE30_V: Interval Accounting

SMF Types Monitored by VSA

- Record Type 32 (20) -- Termination of TSO Session (Often = 30)
- Record Type 42 (2A) – System Managed Storage (SMS) PDS/E activity
  - Subtype 20 – STOW initialization (delete all members)
  - Subtype 21 – Delete member
  - Subtype 24 – Add or Replace member
  - Subtype 25 – Rename member
- Record Type 62 (3E) – VSAM OPEN
- Record Type 80 (50) -- RACF Security (Events 1-89; DataTypes 1-438)
- Record Type 81 (51) – RACF Initialization and SETOPTS
- Record Type 83 (53) -- RACF Security Audit Records

SMF Types Monitored by VSA

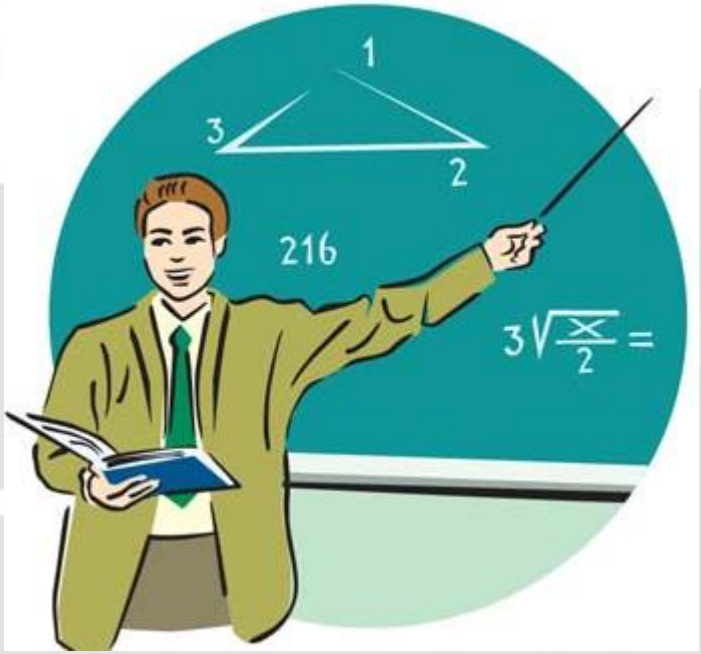
- Record Type 90 (5A) Changes to APF Authorized Library List(z/OS 2.2)
- Record Type 92 (5C) -- Open/MVS File System activity
  - Subtype 1 - when a file system is mounted
  - Subtype 2 - after the file system is quiesced or suspended
  - Subtype 4 - after the file system is unquiesced or resumed
  - Subtype 6 - when the file system is remounted
  - Subtype 7 - when the file system is moved
  - Subtype 10 - when a file is opened
  - Subtype 11 - when a file is closed
  - Subtype 12 - MMAP subtype information
  - Subtype 13 - MUNMAP subtype information
  - Subtype 14 - File/directory delete
  - Subtype 15 - Security attributes changed
  - Subtype 16 - Socket/char spec close (same as 11)
  - Subtype 17 - File accesses

SMF Types Monitored by VSA

- Record Type 102 (66) - DB2 Database Audit (Classes 1-11; Admin actions)
- Record Type 109 (6D) – SyslogD
- Record Type 119 (76) - TCP/IP, Telnet,FTP, FTP Client, UDP Close, TN3270
  - TCPTerm 2 - TCP Connection Termination
  - FTPClient 3 - FTP Client Transfer Completion
  - StackSS 8 - TCP/IP Stack Start/Stop
  - UDPClose A - UDP Socket Close
  - TNSvrTerm 15 - TN3270 Server SNA Session Termination
  - TSOCTerm 17 - TSO Telnet Client Connection Termination
  - FTPServer 46 - FTP Server Transfer Completion
  - FTPLogonF 48 - FTP Server Logon Failure

Demonstration of SMF Events sent to QRadar and Splunk

AND SMF Granular Filtering



Suggested SMF Events to Monitor
Input from existing SDS VSA customers

Questions

(800) 443-6183,
(763) 571-9000

info@sdsusa.com

www.sdsusa.com