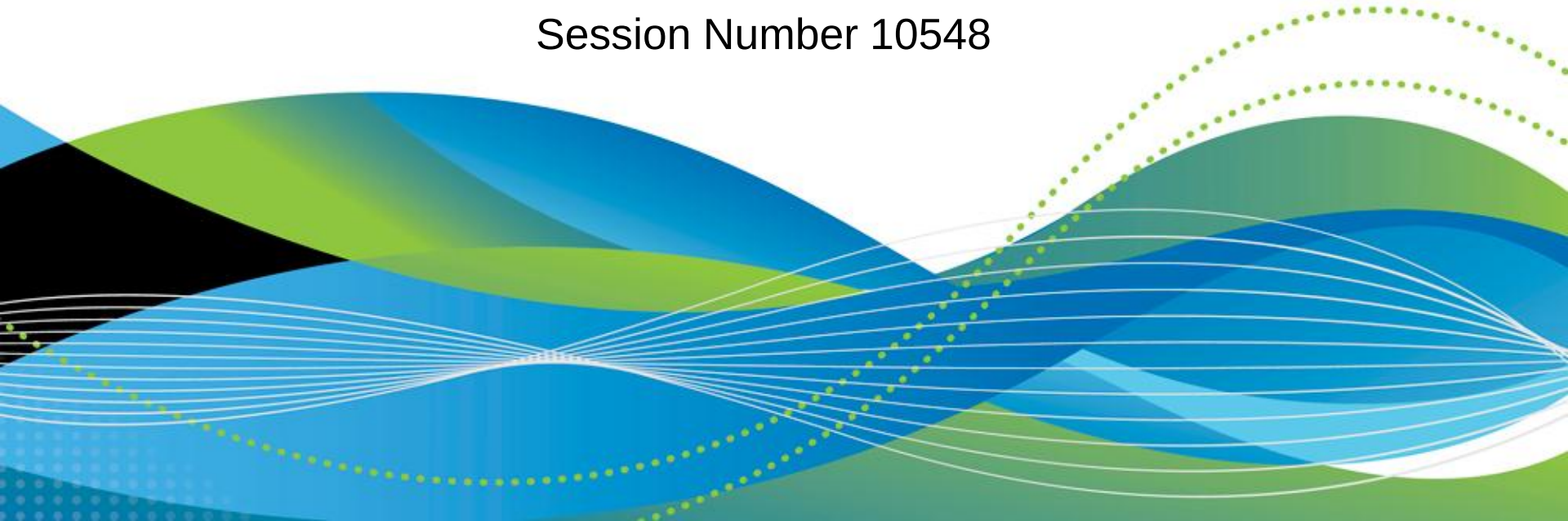
#SHAREorg

SHARE
Technology · Connections · Results

The Truth About FTP And Why It Is Not Secure

Colin van der Ross
Software Diversified Services

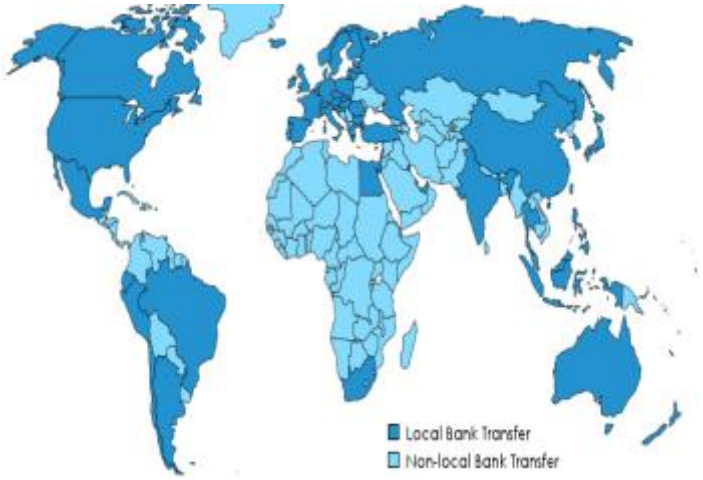
March 14th 2012
Session Number 10548



Agenda

- FTP Today and in the Workplace
- Security Breaches and Compliance
- Risks associated with FTP
- Options to Secure FTP

FTP Today



- Been around since 1971 (before TCP and IP protocols – very aged protocol)
- Millions of critical files and data exchanged by corporations daily
- Few Managers realize the Security and Management Risks with the prevalent use of FTP
- FTP has not “evolved” over the years and is rife with Security Exposures

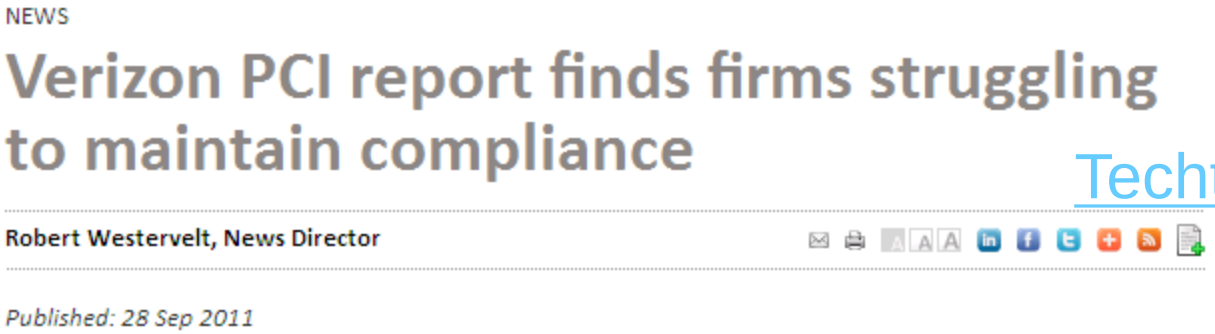
FTP in the Workplace

- Most Computers have the ability to exchange data (Users desktop)
- Embedded in services of TCP/IP
- Business to Business FTP transfers are uncontrolled and insecure
- Critical Lynchpin in Business to Business Communications
- Facility used for file transfers between diverse computing platforms
- The manner in which the way FTP is implemented by Business needs attention
- FTP activity is Rampant. Do you really know what is happening ?

FTP and Compliance – Recently in the News

www.net-security.org

www.healthcareinfosecurity.com



Techtarget.com/news/

FTP and Compliance

1. PCI-DSS

1. Any time credit card information is sent it must abide by the PCI-DSS compliance standards for security and confidentiality.

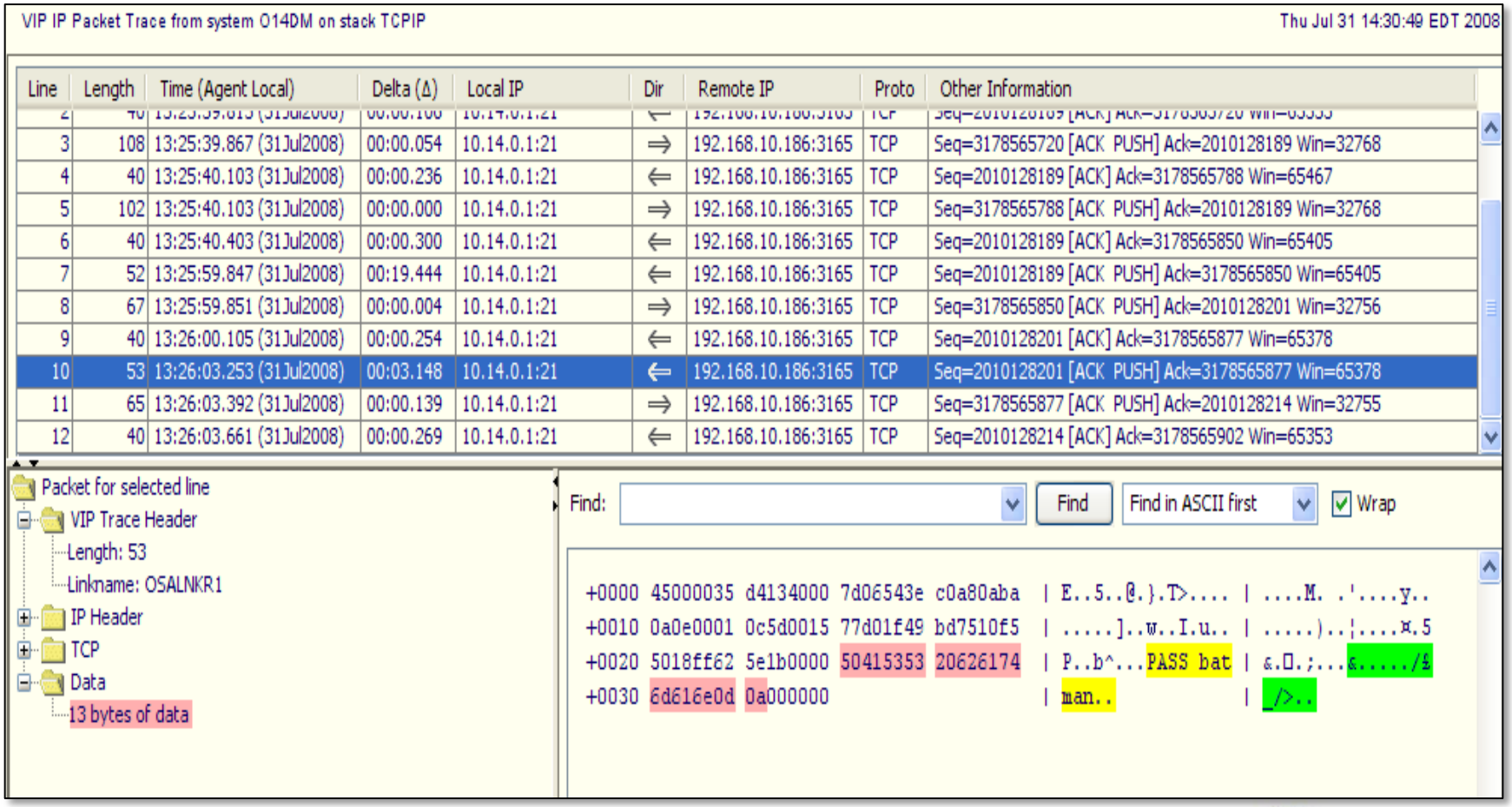
2. HIPAA, SOX, GLBA, FISMA & Others

1. **HIPAA** - The HIPAA Security Rule mandates health plan providers, healthcare clearing houses, and other organizations processing health information to take reasonable and appropriate precautions to protect health information.
2. **SOX** - Section 404 of SOX requires top management to establish an adequate internal control structure and include an assessment of its effectiveness in the annual report. Additionally, an external auditor needs to verify the management assertions.
3. **GLBA** - The Safeguards Rule issued by the Federal Trade Commission (FTC) is established standards for financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect security, confidentiality, and integrity of customer information
4. **FISMA** - FIPS 140-2 requires certified cryptographic modules to meet the compliance requirements for government agencies and certain contractors
5. **California SB 1386**, **Basel II, Massachusetts Privacy Law**

Risks associated with FTP

- Anyone with READ access, also has “Transfer Out” access
- Read Clear Text Exposure
- Password interception
- Eavesdropping
- Hijacking
- “Man in the middle”
- Connection “hijack”
- Spyware
- Wireless Connectivity
- Can open portal behind firewall

FTP Packet Trace Example



Passwords are in the CLEAR

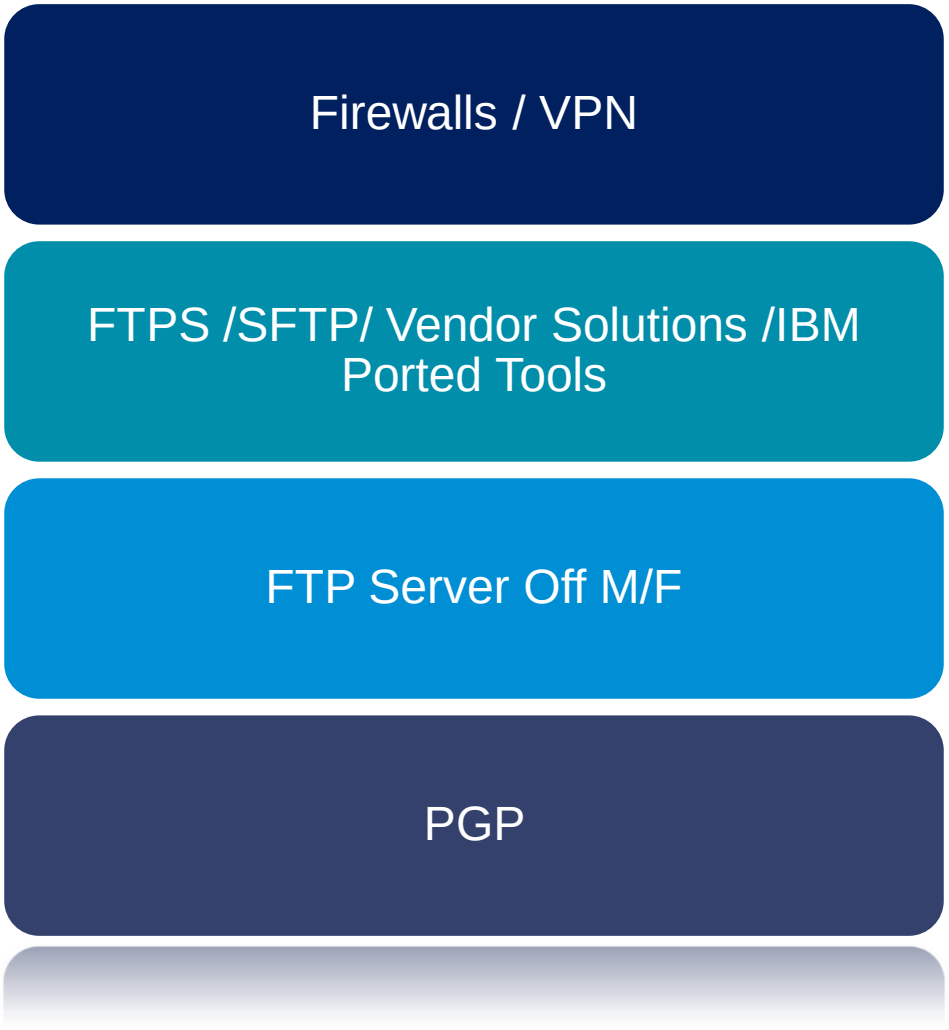
VIP IP Packet Trace from system O14DM on stack TCPIP — Thu Jul 31 14:30:49 EDT 2008

Line	Length	Time (Agent Local)	Delta (Δ)	Local IP	Dir	Remote IP	Proto	Other Information
3	108	13:25:39.867 (31Jul2008)	00:00.054	10.14.0.1:21	⇒	192.168.10.186:3165	TCP	Seq=3178565720 [ACK PUSH] Ack=2010128189 Win=32768
4	40	13:25:40.103 (31Jul2008)	00:00.236	10.14.0.1:21	⇐	192.168.10.186:3165	TCP	Seq=2010128189 [ACK] Ack=3178565788 Win=65467
5	102	13:25:40.103 (31Jul2008)	00:00.000	10.14.0.1:21	⇒	192.168.10.186:3165	TCP	Seq=3178565788 [ACK PUSH] Ack=2010128189 Win=32768
6	40	13:25:40.403 (31Jul2008)	00:00.300	10.14.0.1:21	⇐	192.168.10.186:3165	TCP	Seq=2010128189 [ACK] Ack=3178565850 Win=65405
7	52	13:25:59.847 (31Jul2008)	00:19.444	10.14.0.1:21	⇐	192.168.10.186:3165	TCP	Seq=2010128189 [ACK PUSH] Ack=3178565850 Win=65405
8	67	13:25:59.851 (31Jul2008)	00:00.004	10.14.0.1:21	⇒	192.168.10.186:3165	TCP	Seq=3178565850 [ACK PUSH] Ack=2010128201 Win=32756
9	40	13:26:00.105 (31Jul2008)	00:00.254	10.14.0.1:21	⇐	192.168.10.186:3165	TCP	Seq=2010128201 [ACK] Ack=3178565877 Win=65378
10	53	13:26:03.253 (31Jul2008)	00:03.148	10.14.0.1:21	⇐	192.168.10.186:3165	TCP	Seq=2010128201 [ACK PUSH] Ack=3178565877 Win=65378
11								
12								

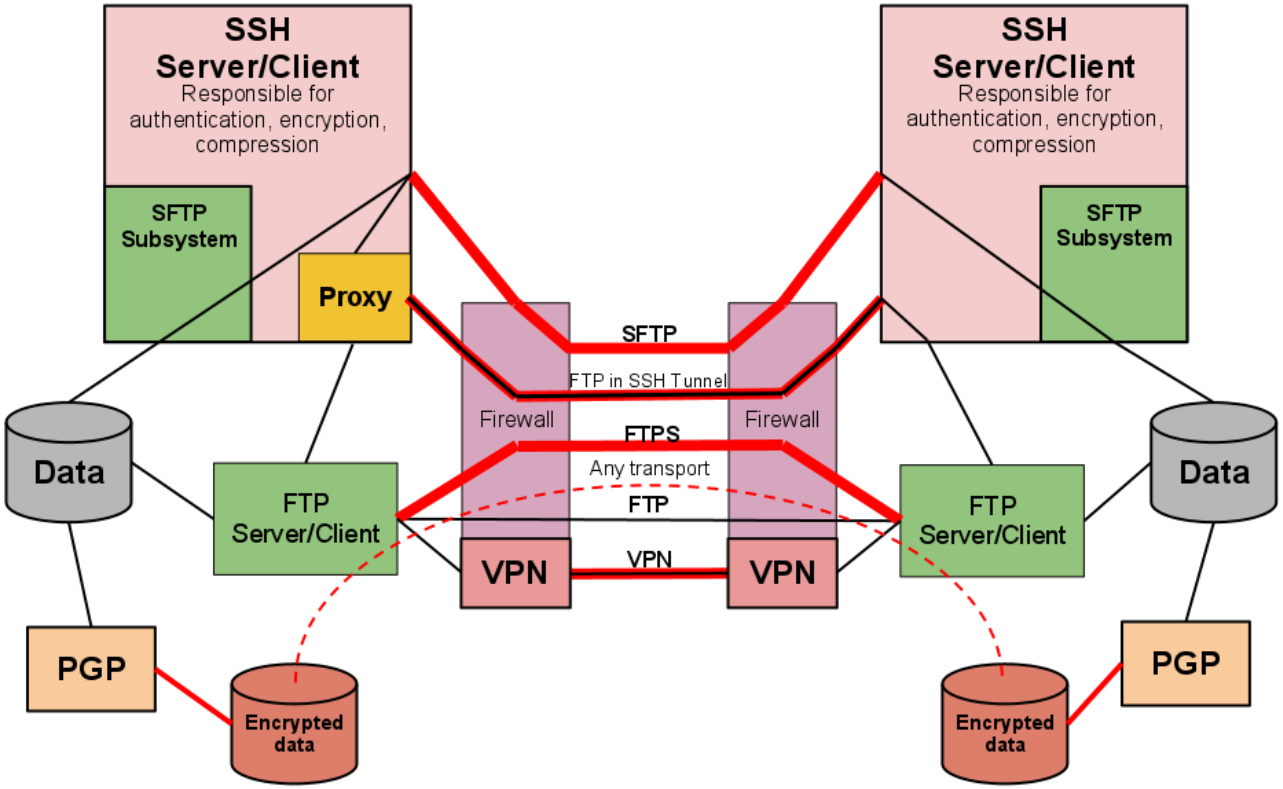
Packet for
VIP Tr
Length
Linkna
IP Hea
TCP
Data
13 byt

```
+0000 45000035 d4134000 7d06543e c0a80aba | E..5..@.}.T>.... | ....M. .'....y..
+0010 0a0e0001 0c5d0015 77d01f49 bd7510f5 | .....]..w..I.u.. | .....)..¦....¤.5
+0020 5018ff62 5e1b0000 50415353 20626174 | P..b^...PASS bat | &.□.;...&...../£
+0030 6d616e0d 0a000000                   | man..            | _/>..
```

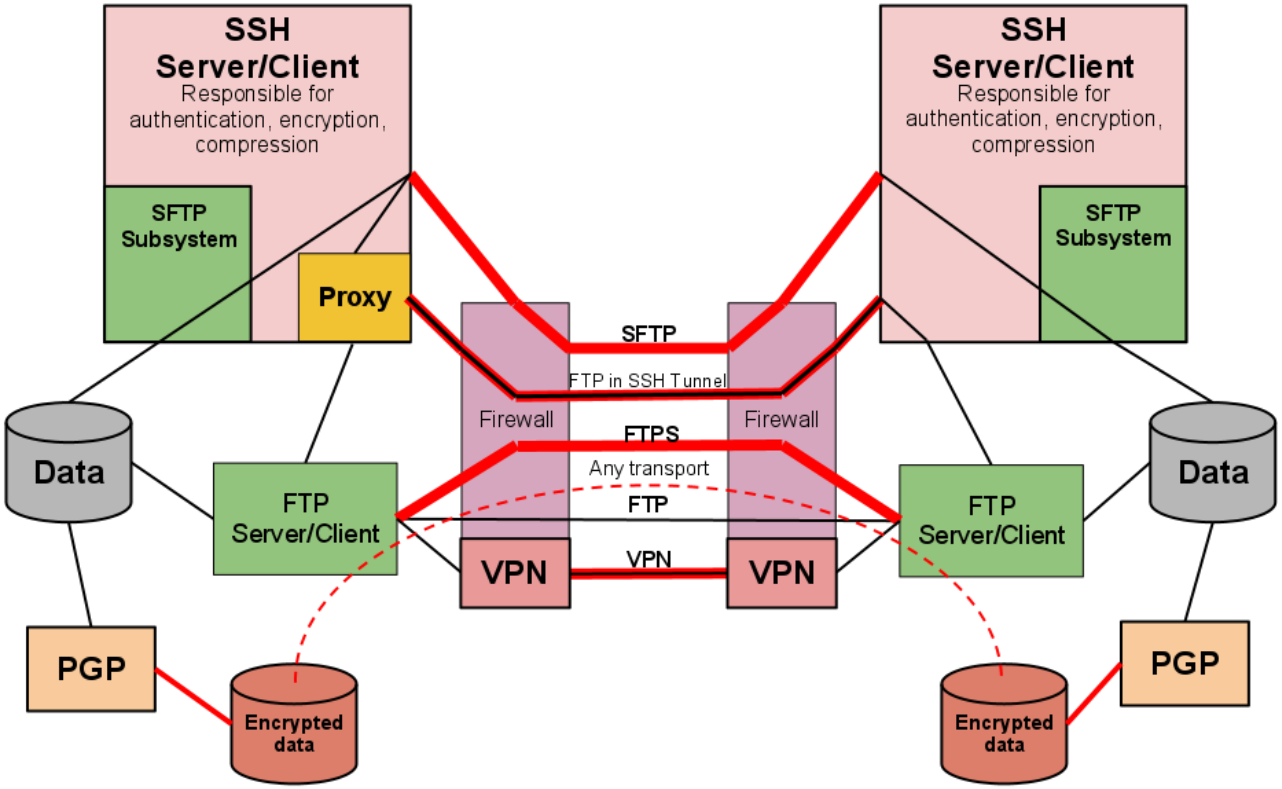
What Are The Options To Secure Your FTP Secure ?



Truth about FTP

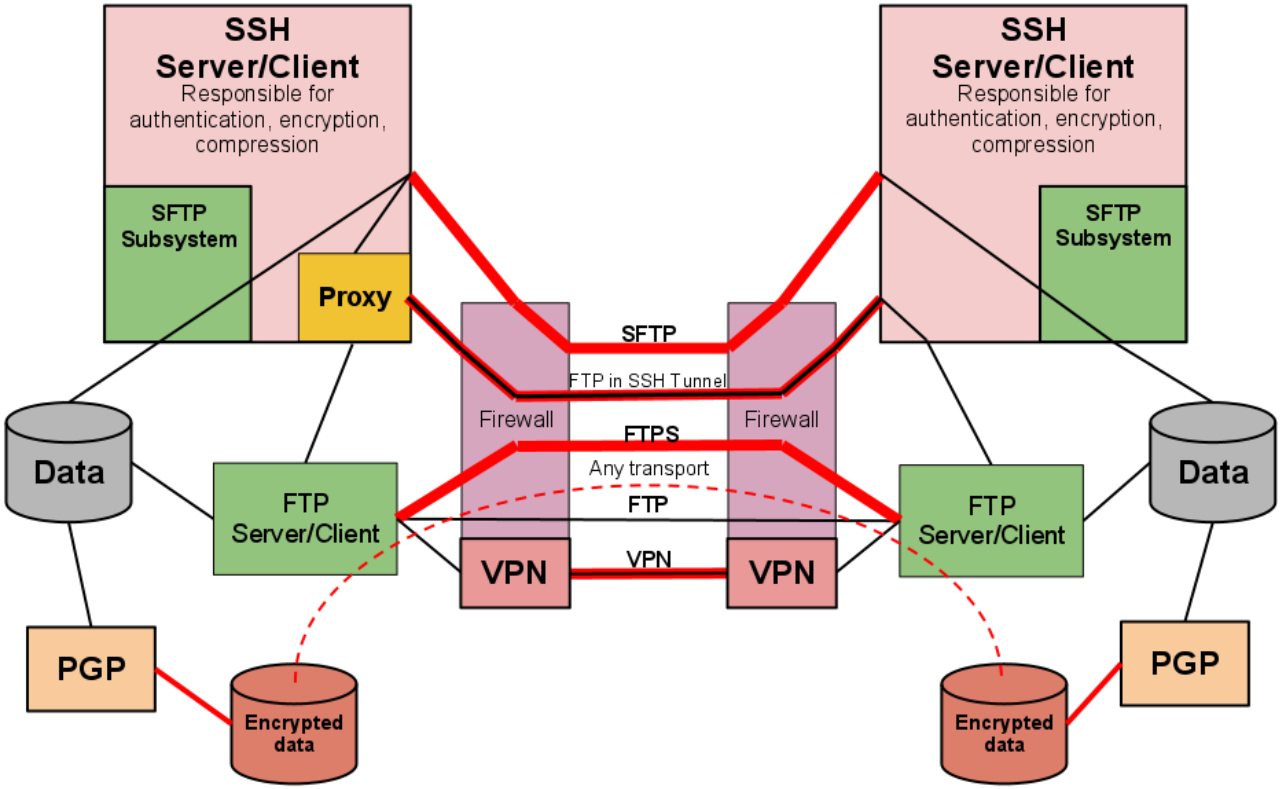


The Truth about FTP



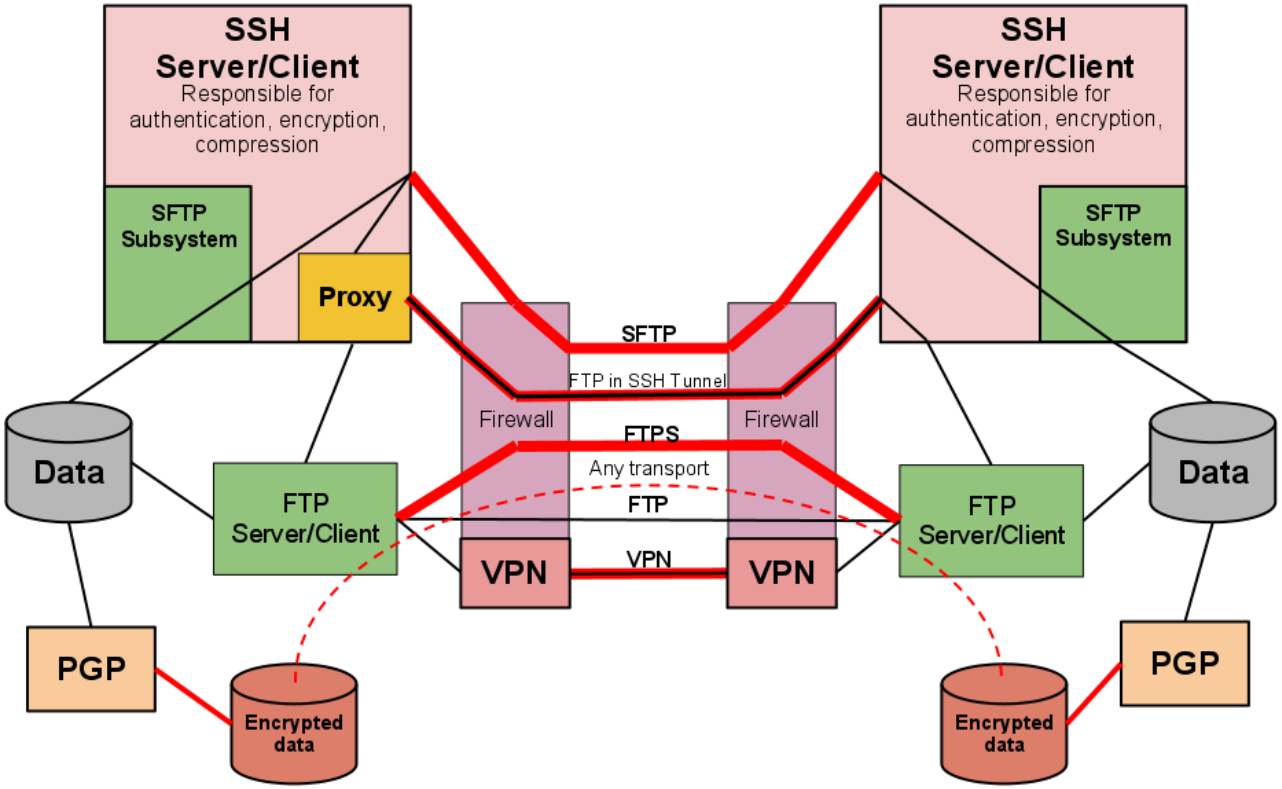
- What are some alternatives

The Truth about FTP



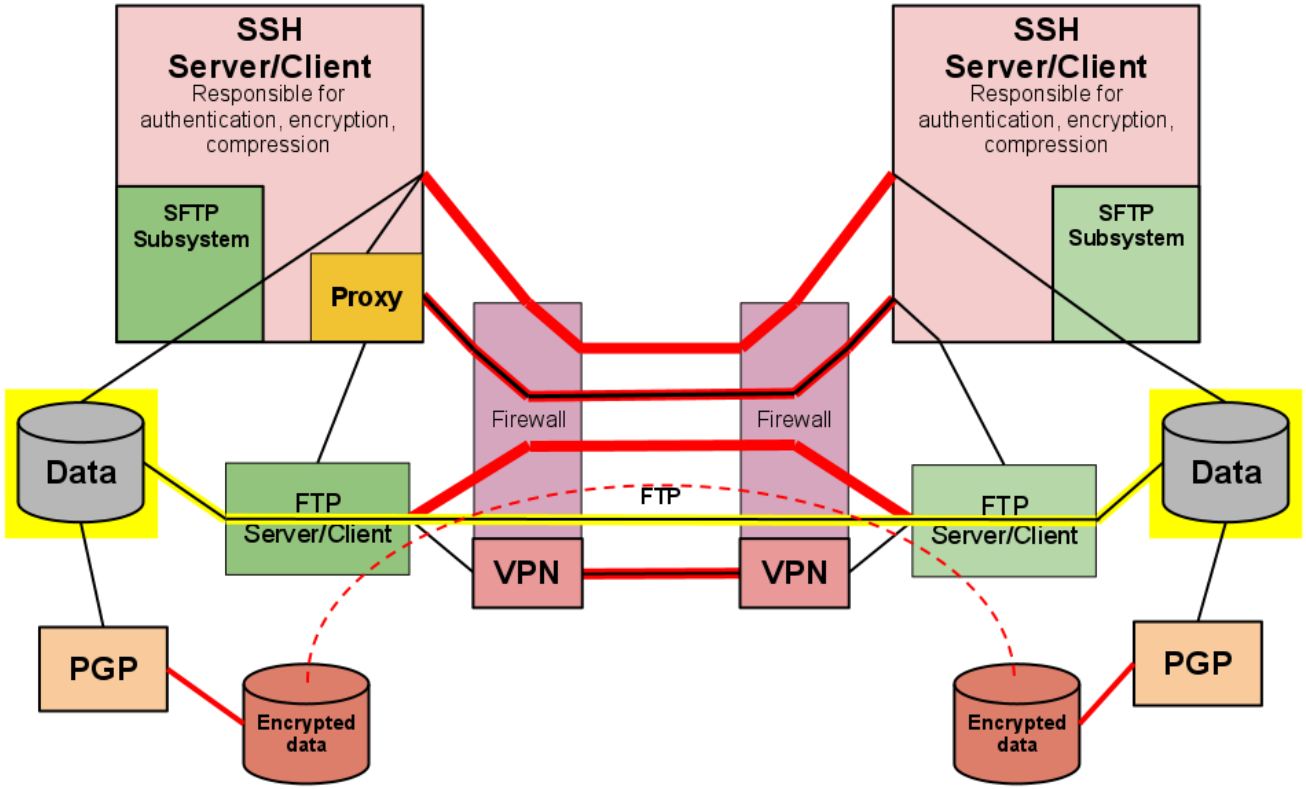
- What are some alternatives
- Why or why not use the methods and tools

The Truth about FTP



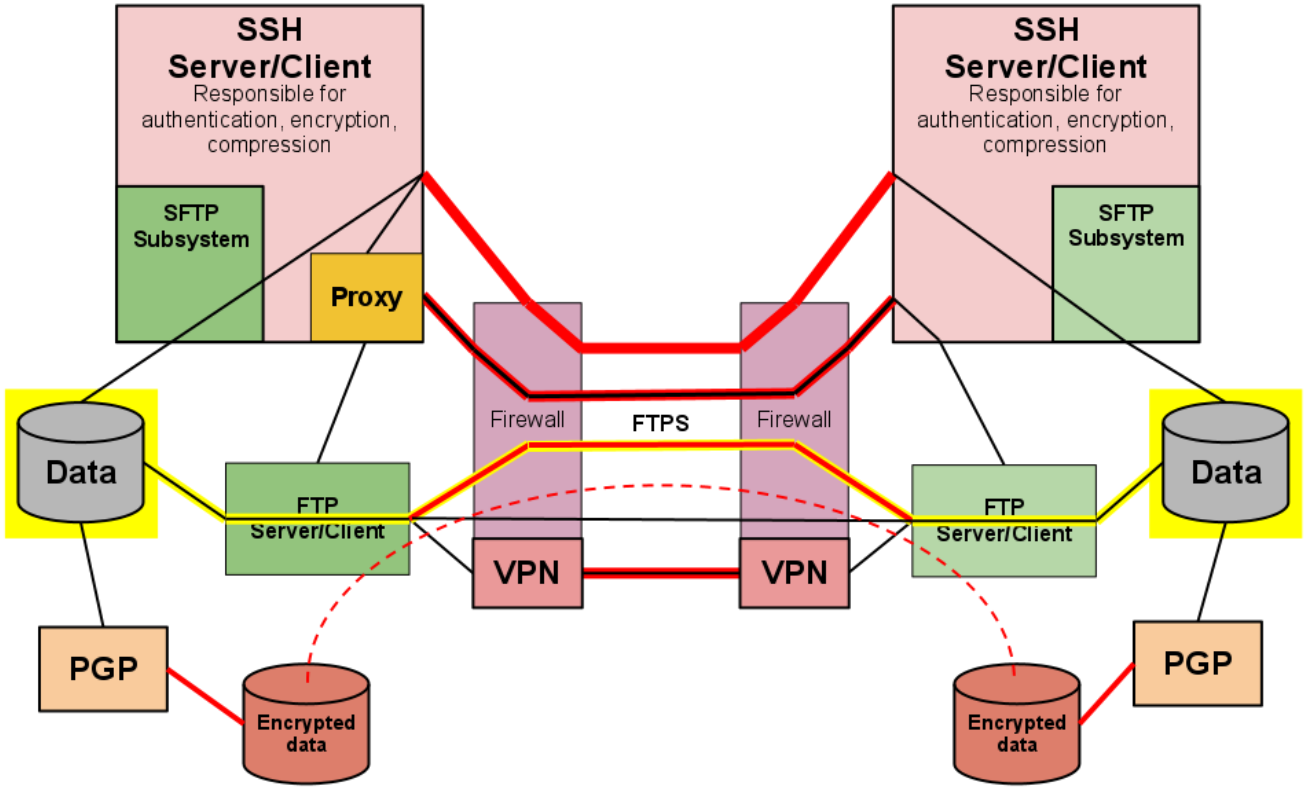
- What are some alternatives
- Why or why not use the methods and tools
- When is a good time to use the solution

FTP (File Transfer Protocol)



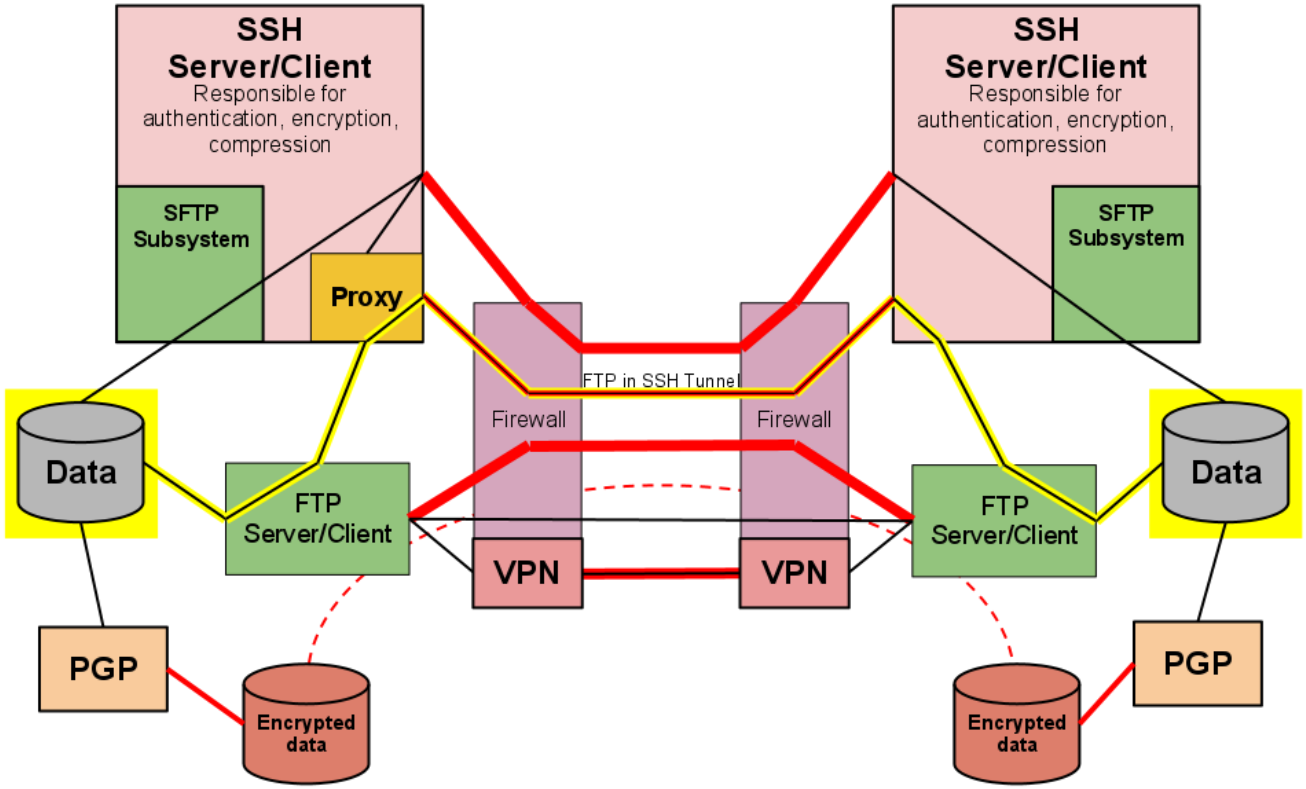
- FTP

FTPS (FTP over SSL)



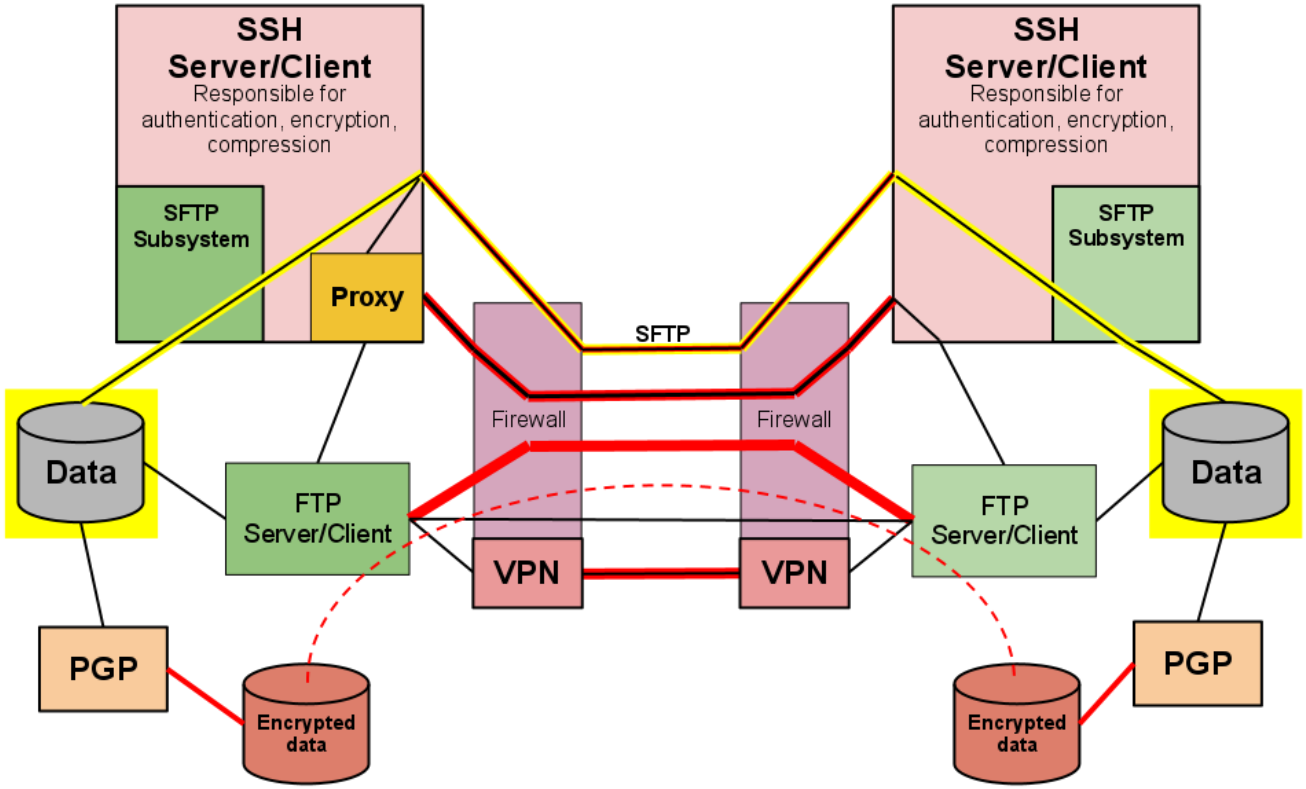
- FTP
- FTPS

FTP over SSH Tunnel



- FTP
- FTPS
- FTP over SSH Tunnel

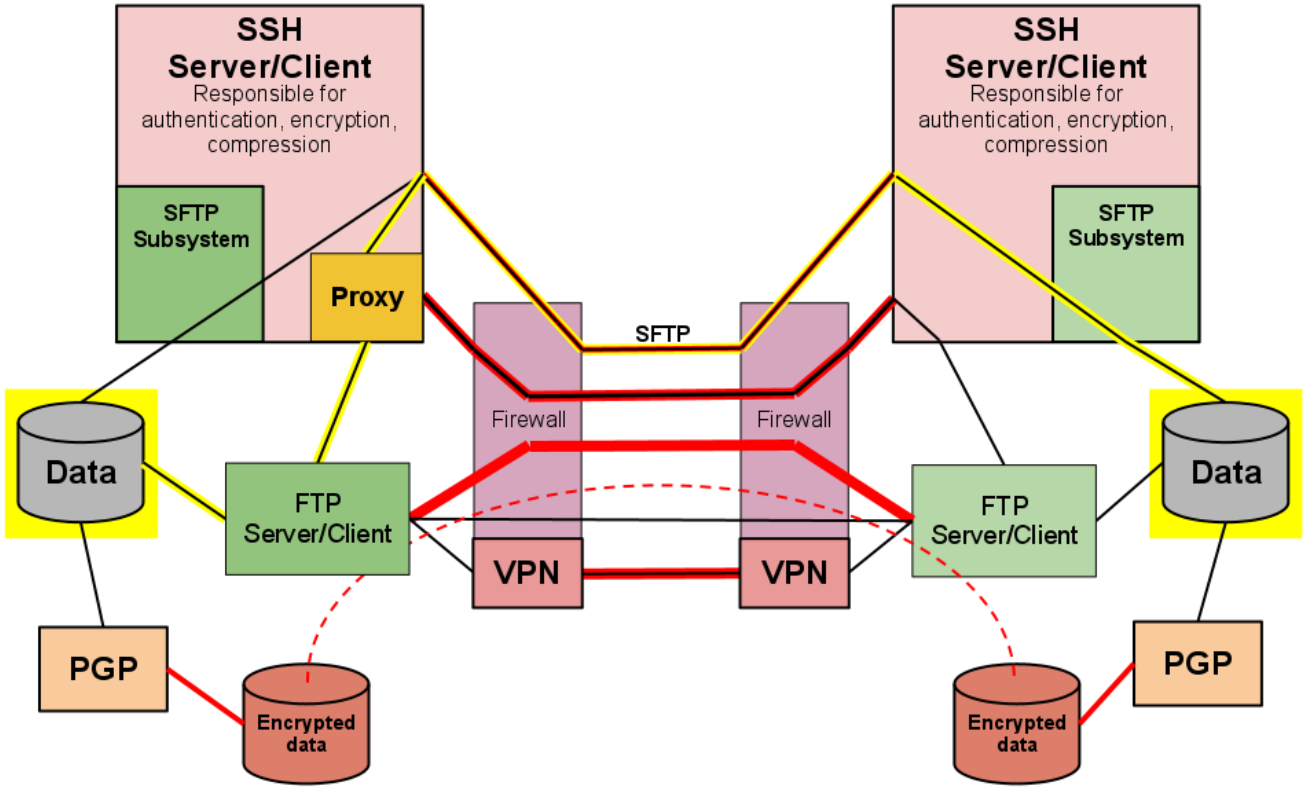
SFTP (SSH Secure FTP)



- FTP
- FTPS
- FTP over SSH Tunnel

- SFTP

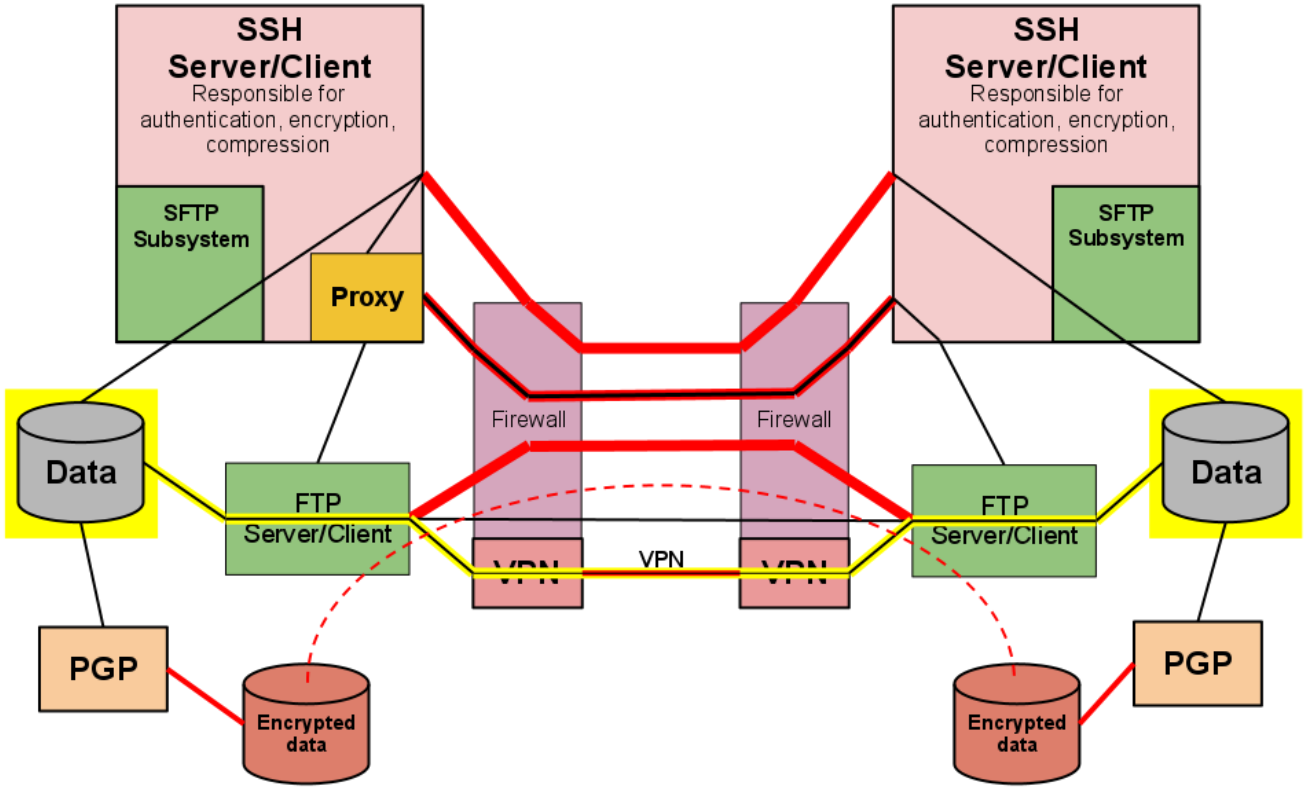
FTP/SFTP Hybrid



- FTP
- FTPS
- FTP over SSH Tunnel

- SFTP
- FTP to SFTP

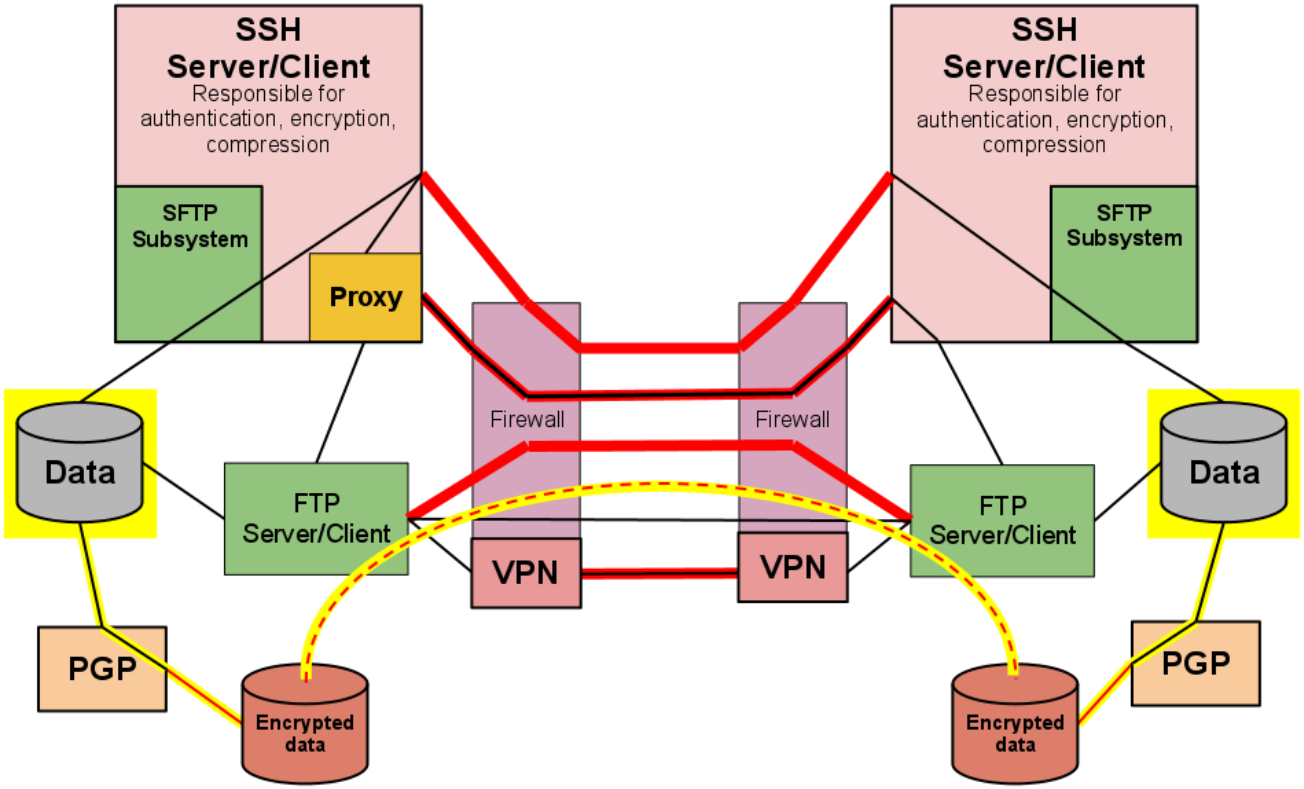
VPN (Virtual Private Network)



- FTP
- FTPS
- FTP over SSH Tunnel

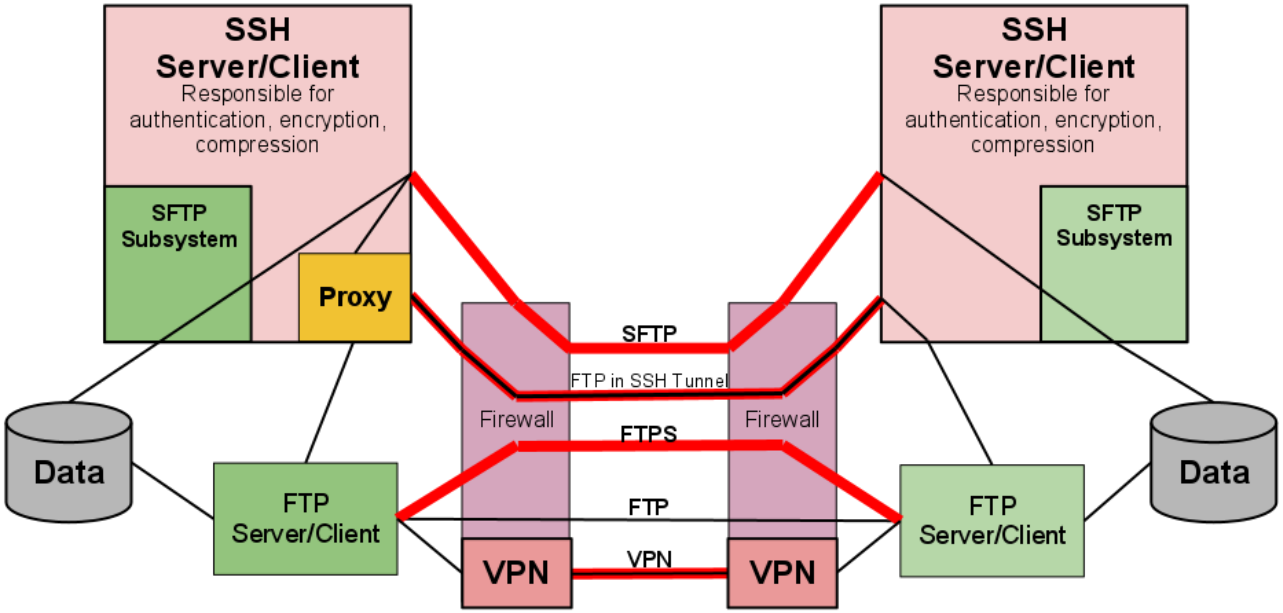
- SFTP
- FTP to SFTP
- VPN

PGP (Data at rest)



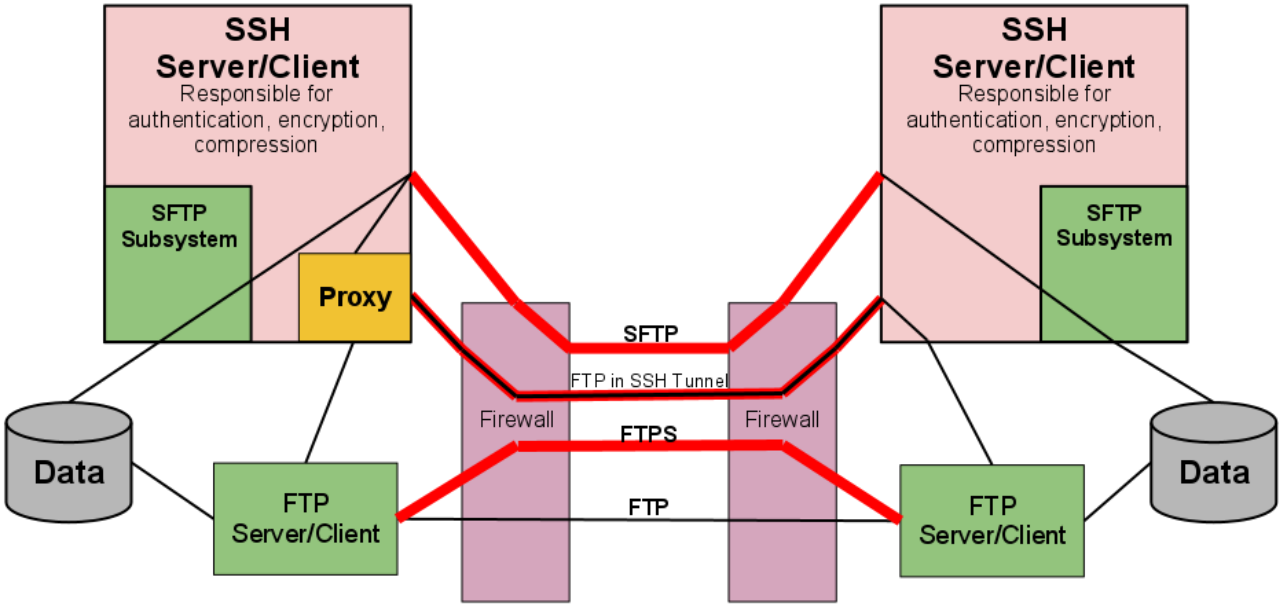
- FTP
- FTPS
- FTP over SSH Tunnel

- SFTP
- FTP to SFTP
- VPN
- PGP



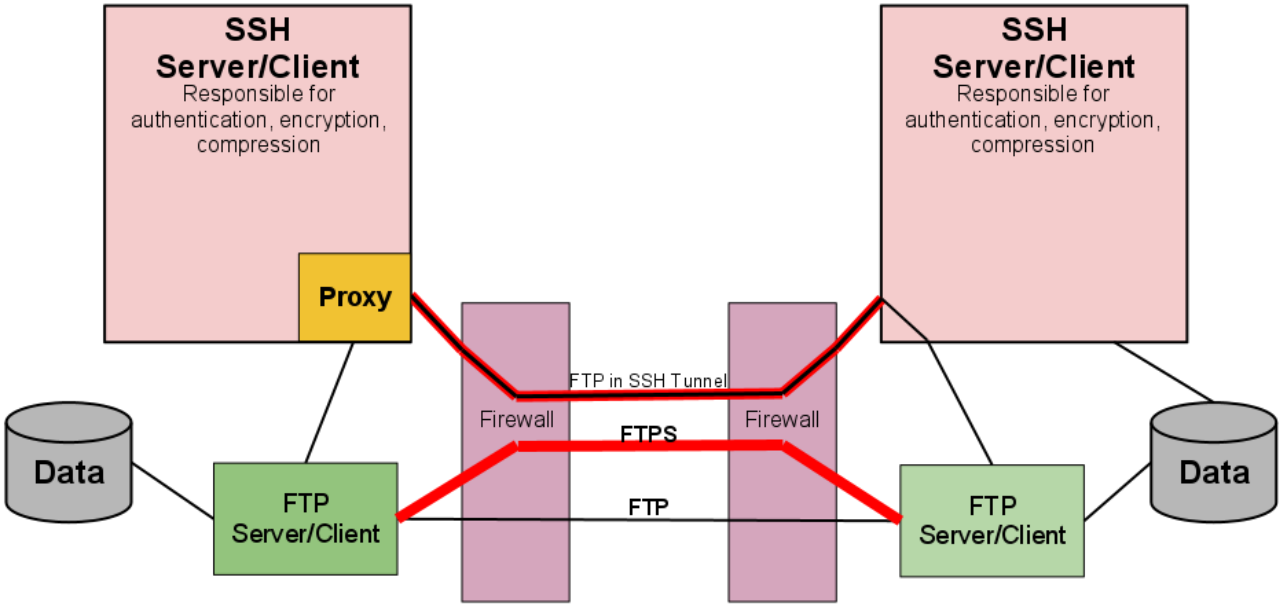
- FTP
- FTPS
- FTP over SSH Tunnel

- SFTP
- FTP to SFTP
- VPN

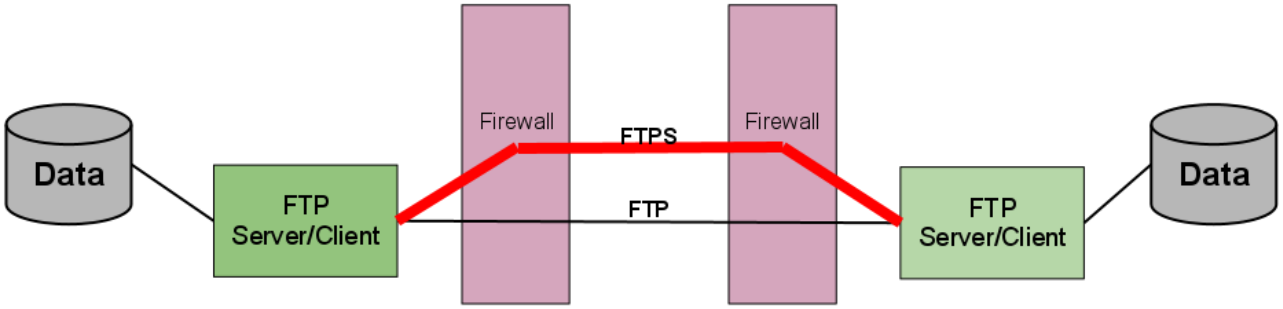


- FTP
- FTPS
- FTP over SSH Tunnel

- SFTP
- FTP to SFTP

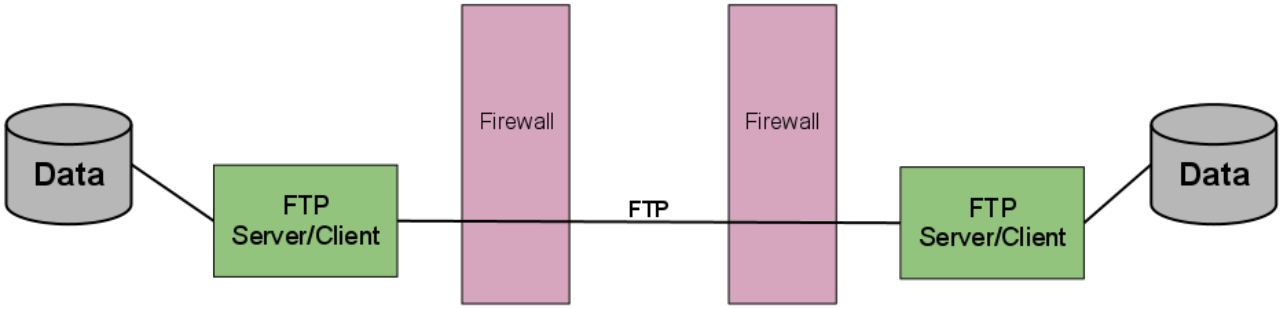


- FTP
- FTPS
- FTP over SSH Tunnel


Data
FTP
Server/Client
Firewall
FTPS
FTP
Firewall
FTP
Server/Client
Data

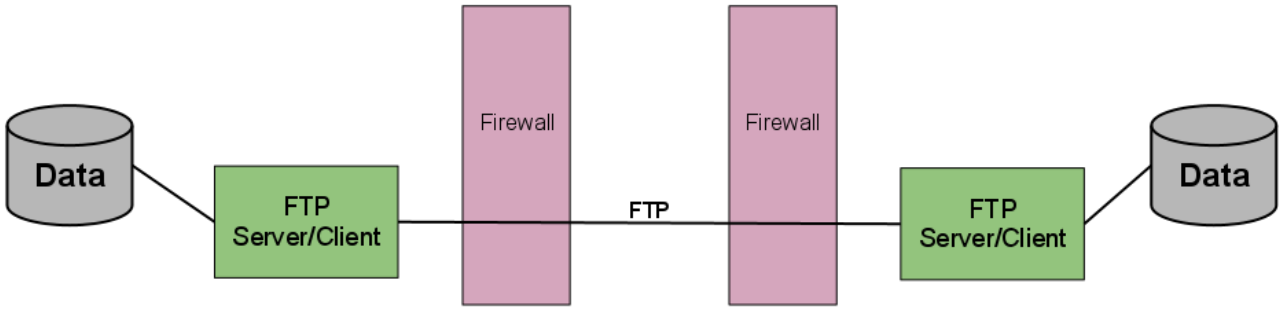
- FTP
- FTPS

FTP



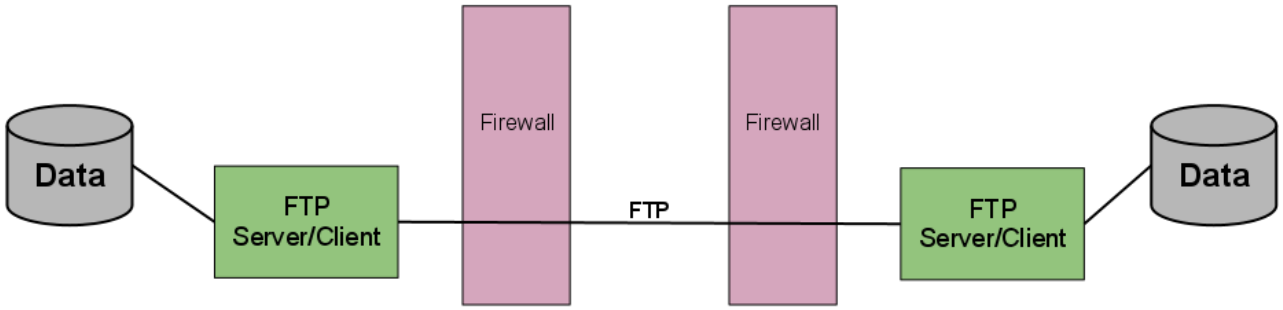
- Pros
  - Ubiquitous

FTP



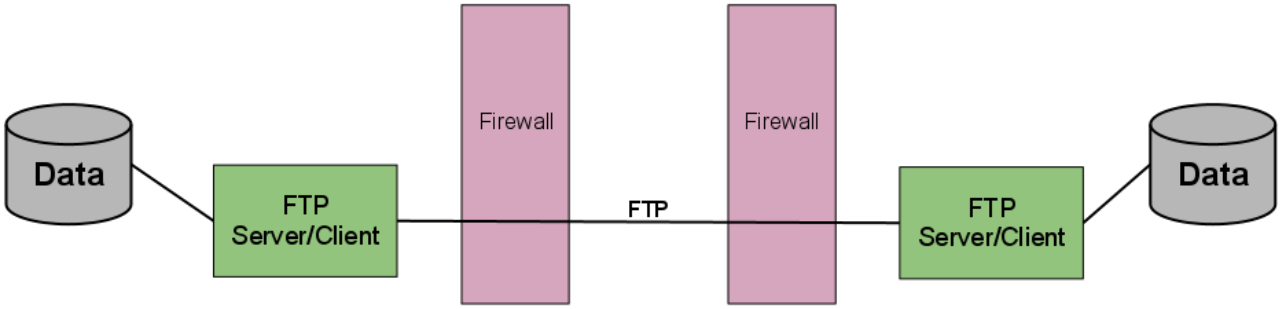
- Pros
  - Ubiquitous
  - Common knowledge

FTP



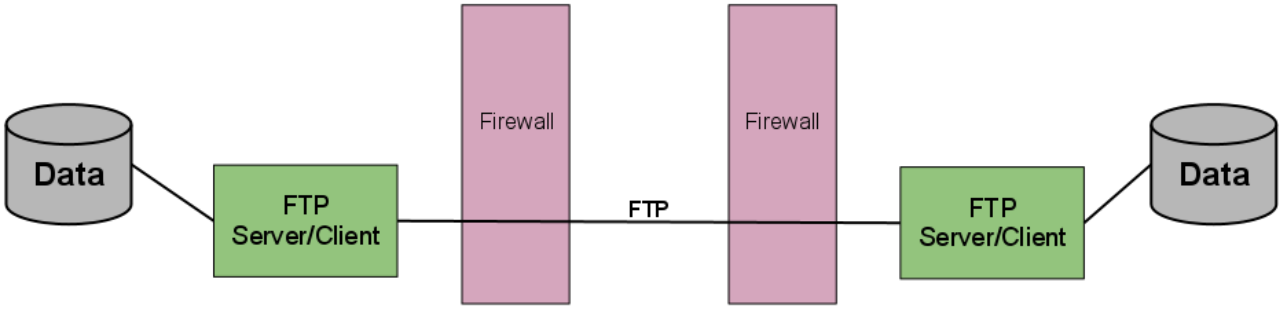
- Pros
  - Ubiquitous
  - Common knowledge
  - Included in base OS

FTP



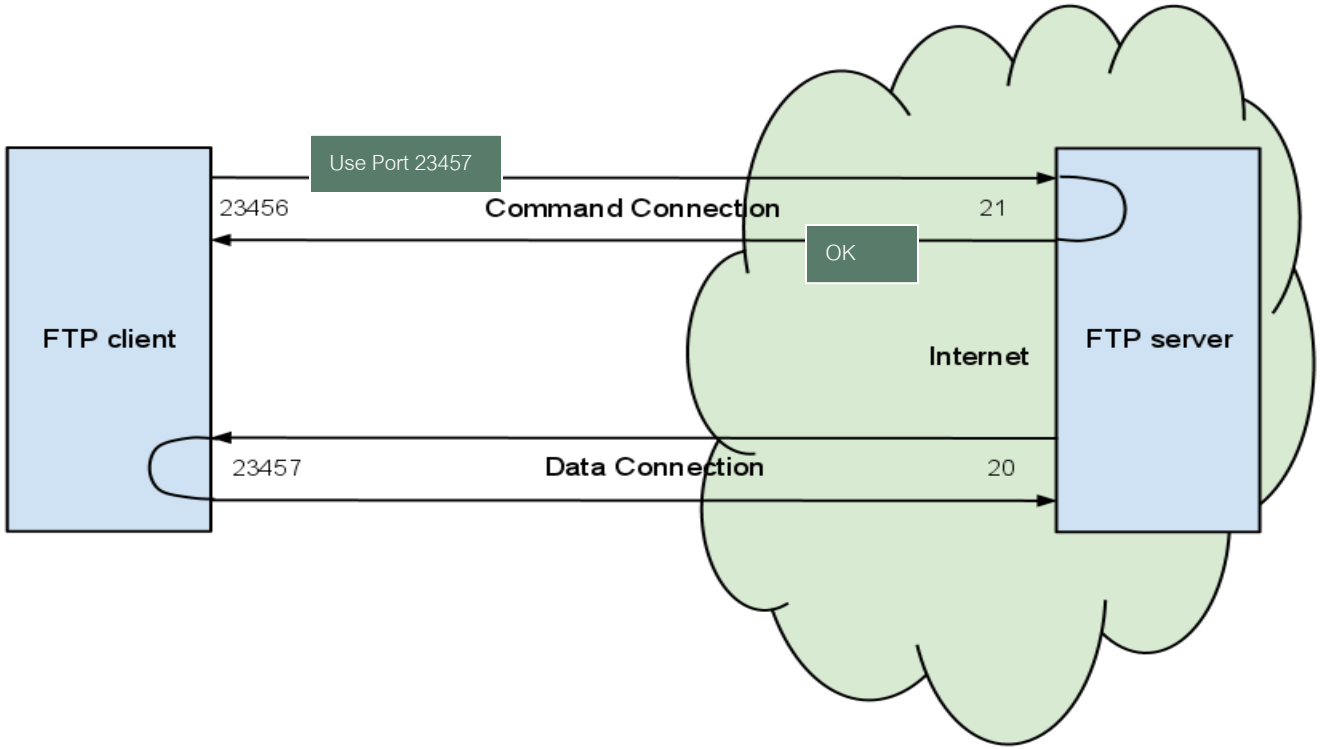
- Pros
  - Ubiquitous
  - Common knowledge
  - Included in base OS
- Cons
  - Very little security

FTP

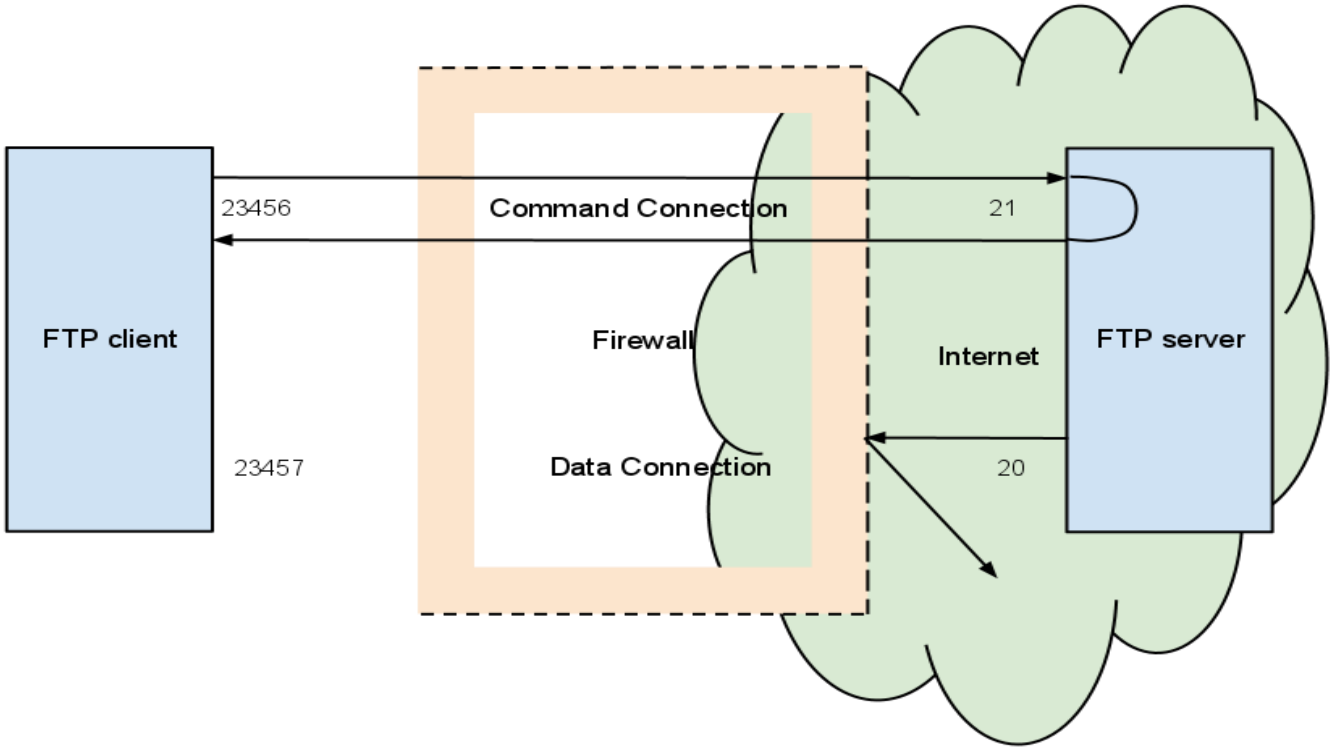


- Pros
  - Ubiquitous
  - Common knowledge
  - Included in base OS
- Cons
  - Very little security
  - Not firewall friendly

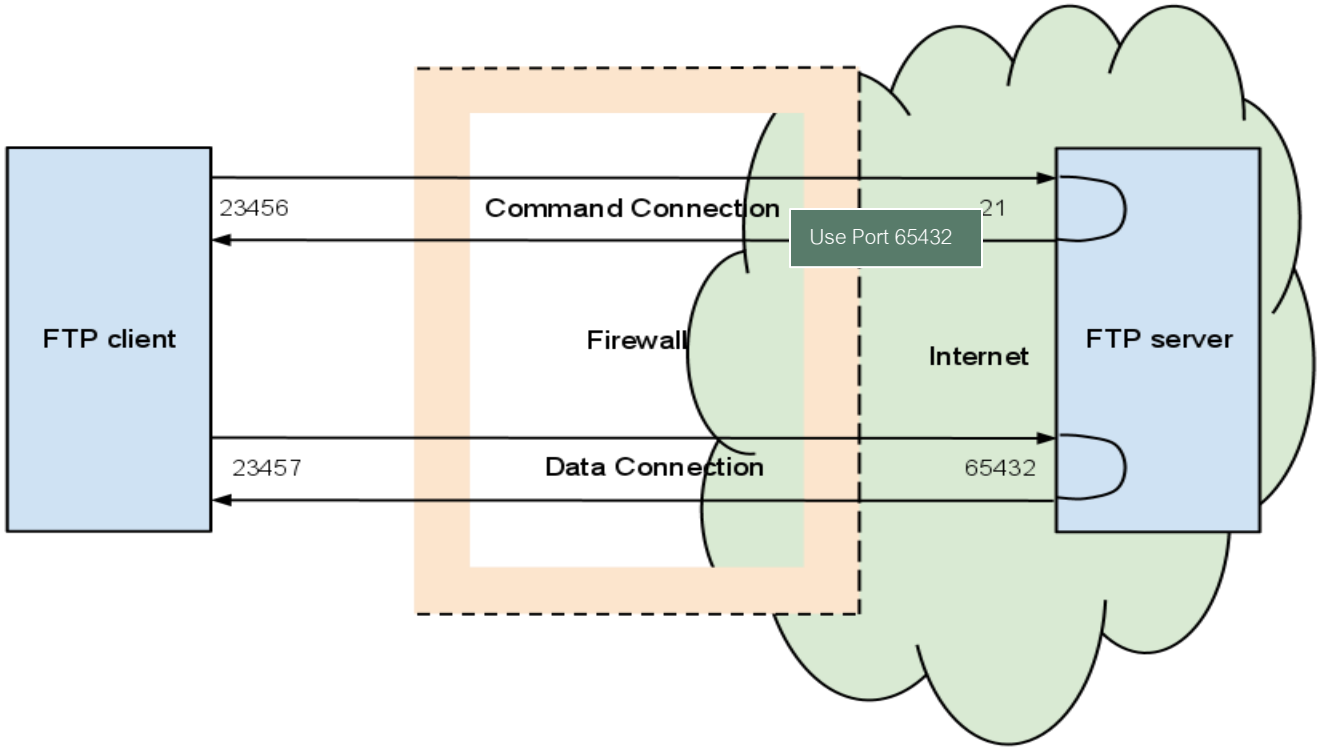
Active Firewall



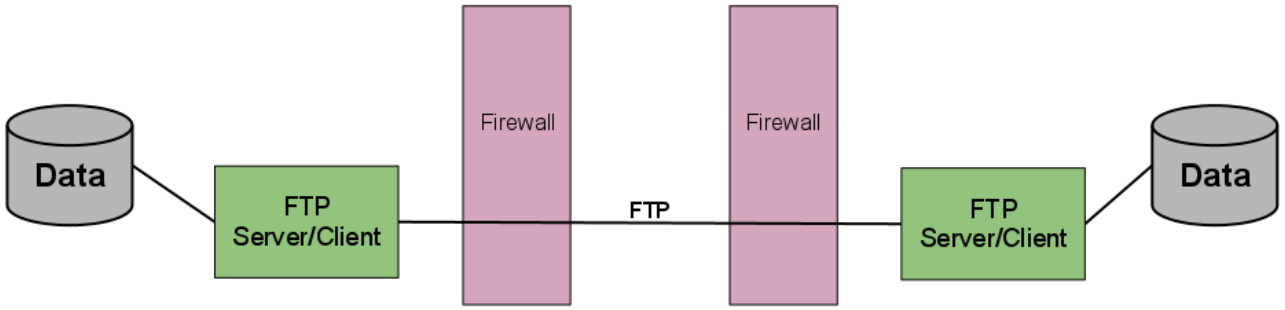
Active FTP with Firewall



Passive FTP

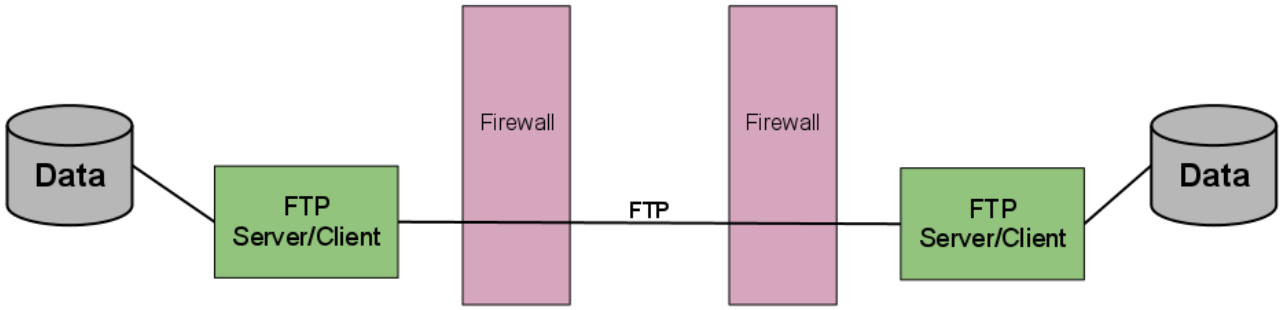

FTP client
23456
Command Connection
21
Use Port 65432
Firewall
Internet
FTP server
23457
Data Connection
65432

FTP



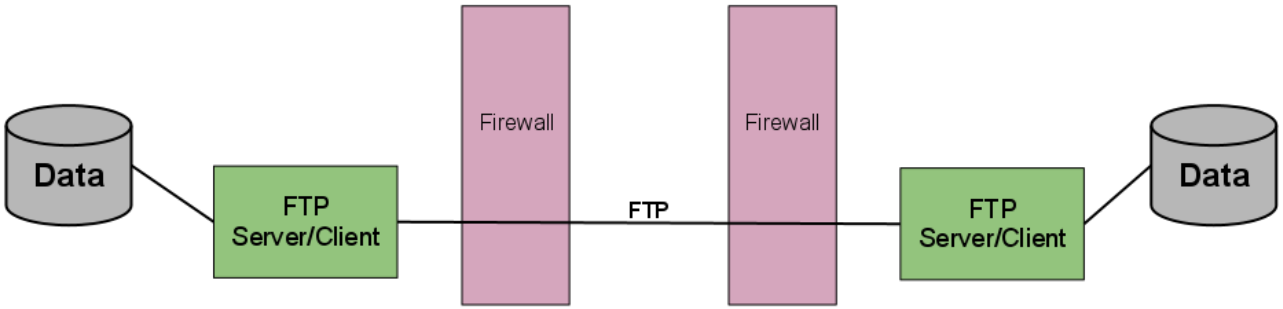
- Pros
  - Ubiquitous
  - Common knowledge
  - Included in base OS
- Cons
  - Very little security
  - Not firewall friendly
  - No native compression

FTP



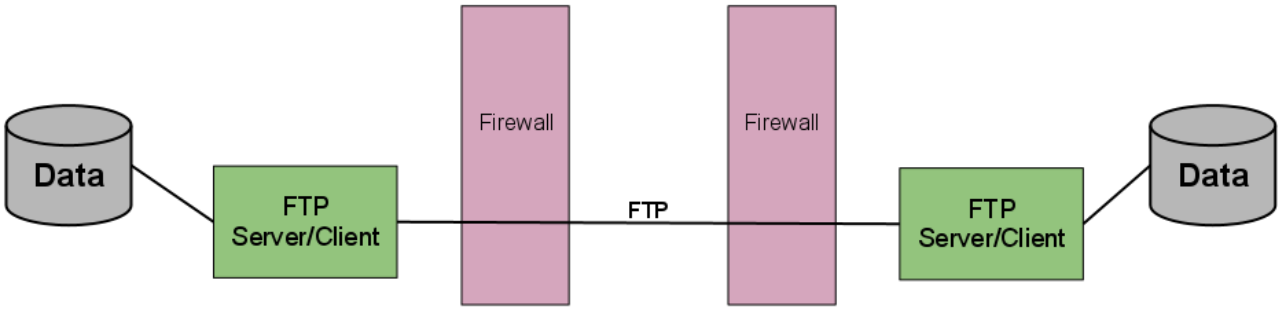
- Pros
  - Ubiquitous
  - Common knowledge
  - Included in base OS
- Cons
  - Very little security
  - Not firewall friendly
  - No native compression
  - Lacks integrity validation

FTP



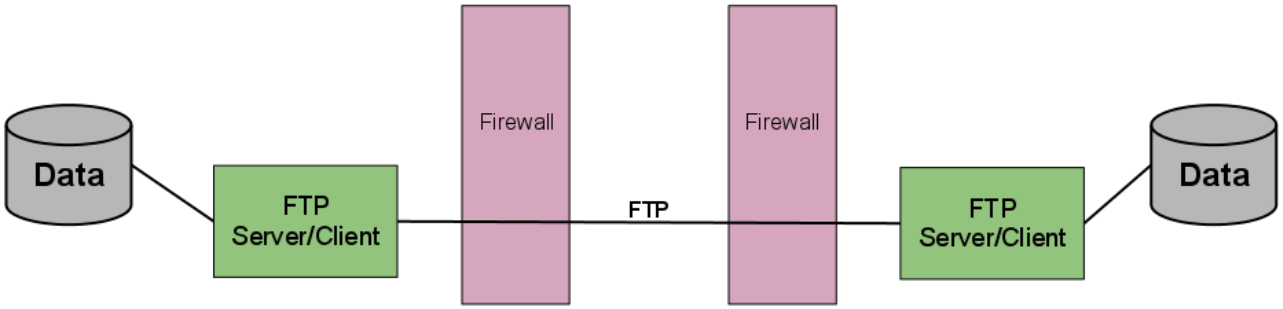
- Common uses
  - Public information

FTP



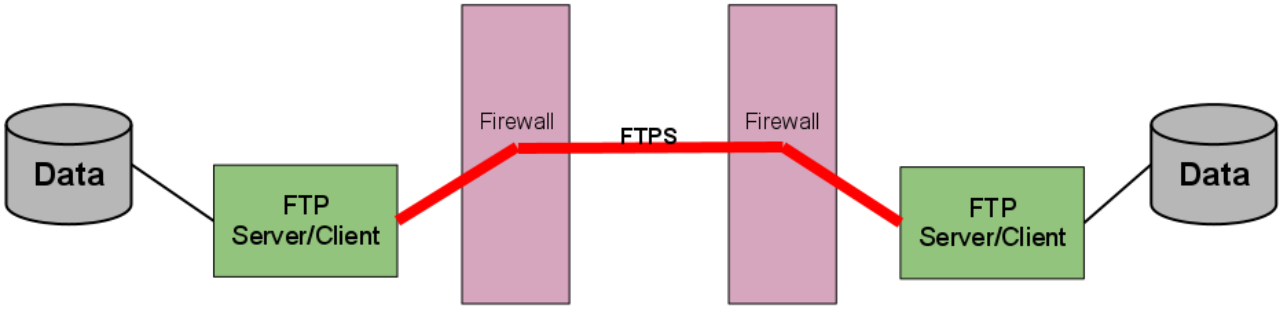
- Common uses
  - Public information
  - Intranet transfers (careful, not everyone on the intranet is safe)

FTP



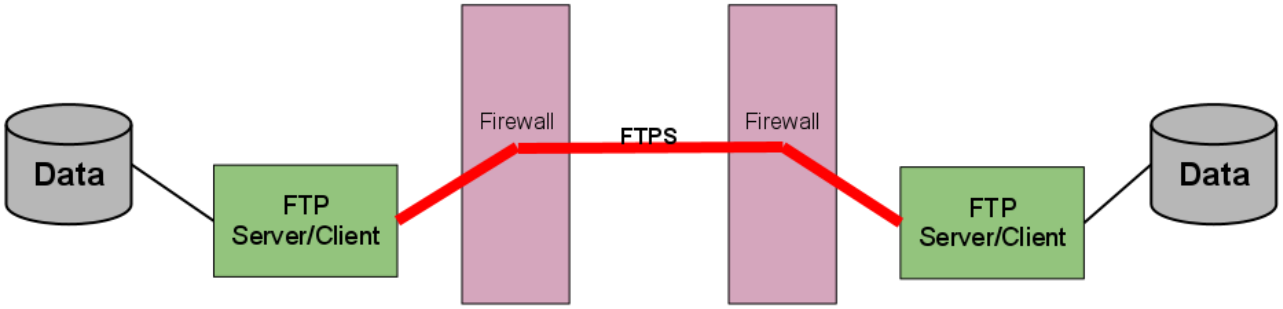
- Common uses
  - Public information
  - Intranet transfers (careful, not everyone on the intranet is safe)
  - Far too many things that should really use something better

FTP over SSL (FTPS)



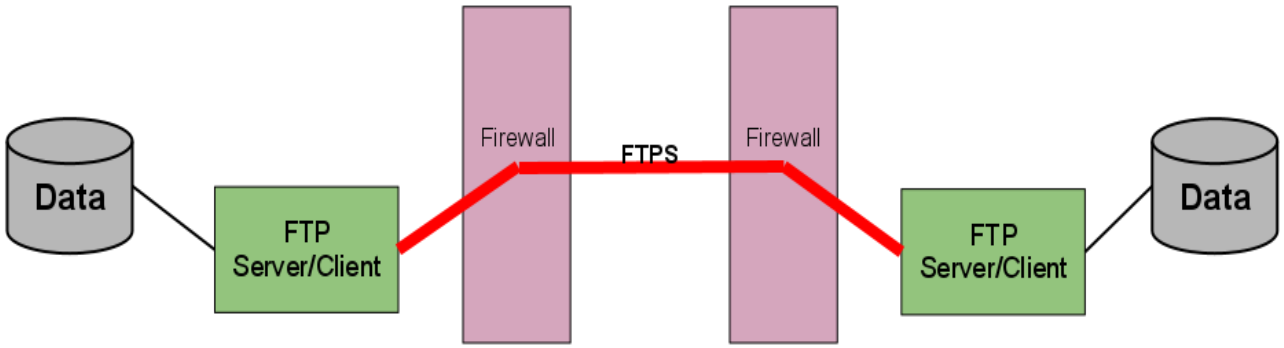
- Pros
  - Same FTP familiarity

FTP over SSL (FTPS)



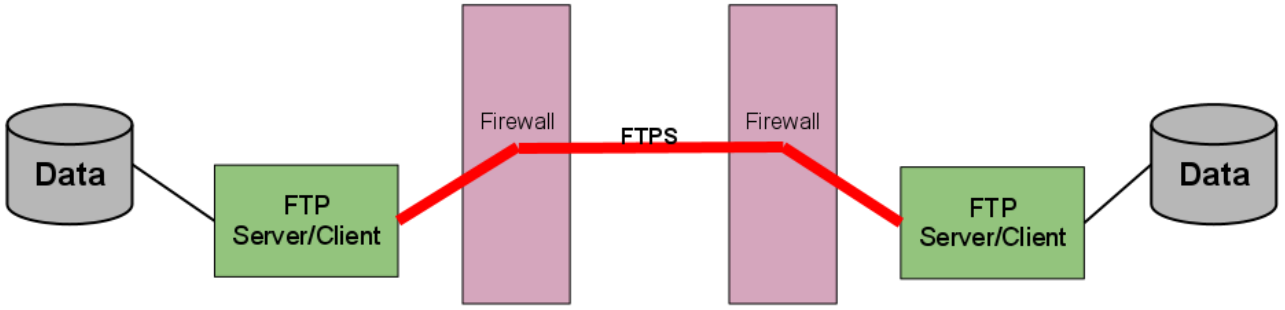
- Pros
  - Same FTP familiarity
  - Included in base z/OS

FTP over SSL (FTPS)



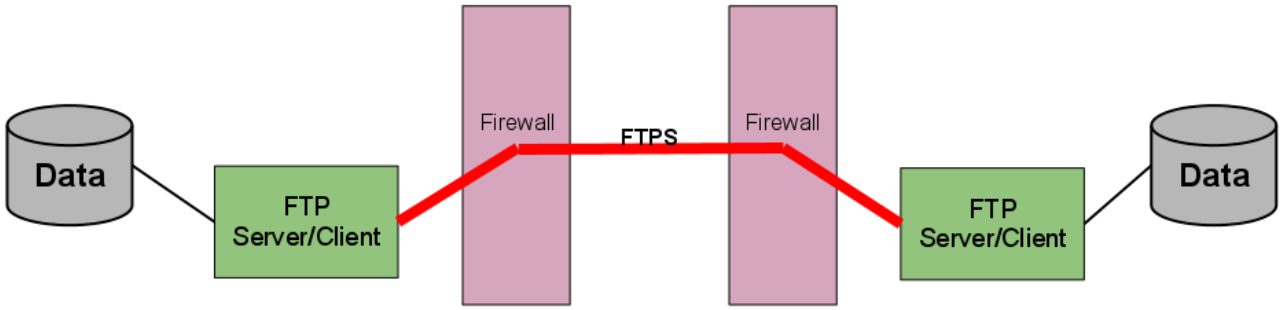
- Pros
  - Same FTP familiarity
  - Included in base z/OS
  - Supports X.509 certificates (trusted authority) and keberos

FTP over SSL (FTPS)



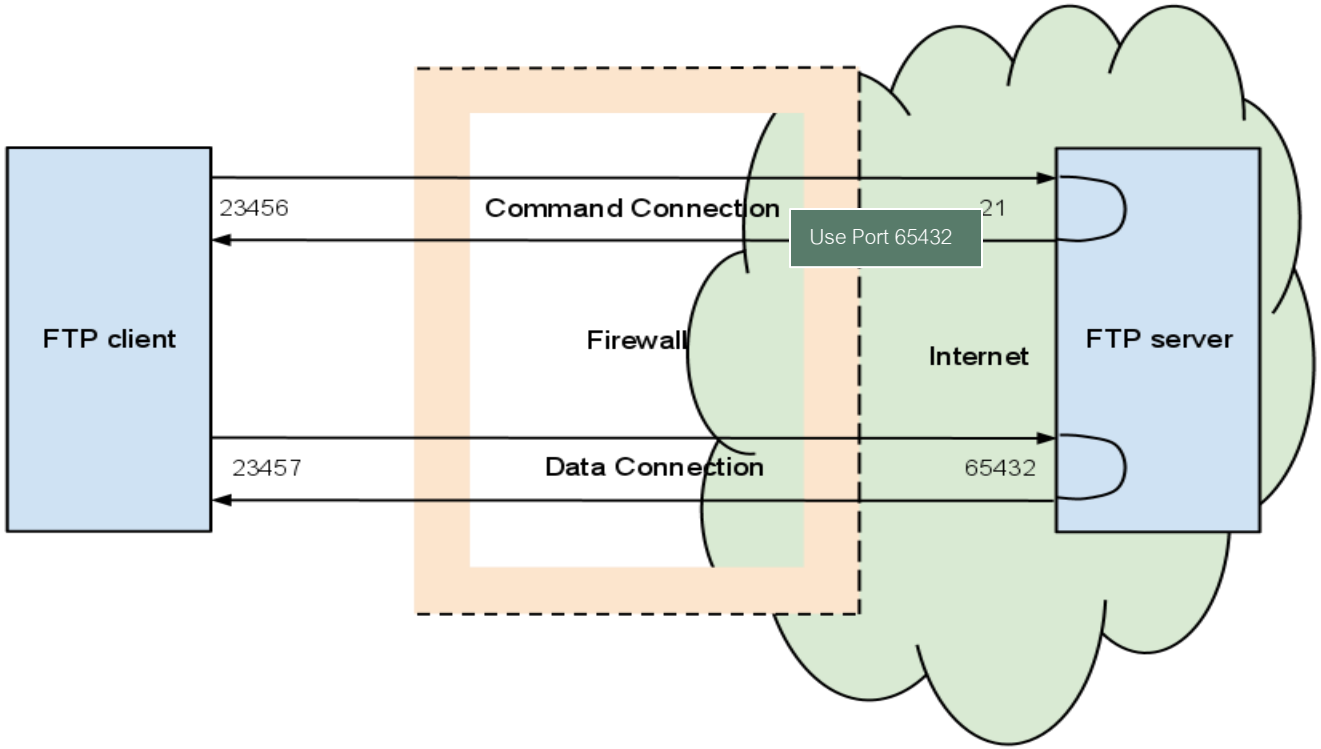
- Pros
  - Same FTP familiarity
  - Included in base z/OS
  - Supports X.509 certificates (trusted authority) and keberos
  - RACF keyrings supported

FTP over SSL (FTPS)

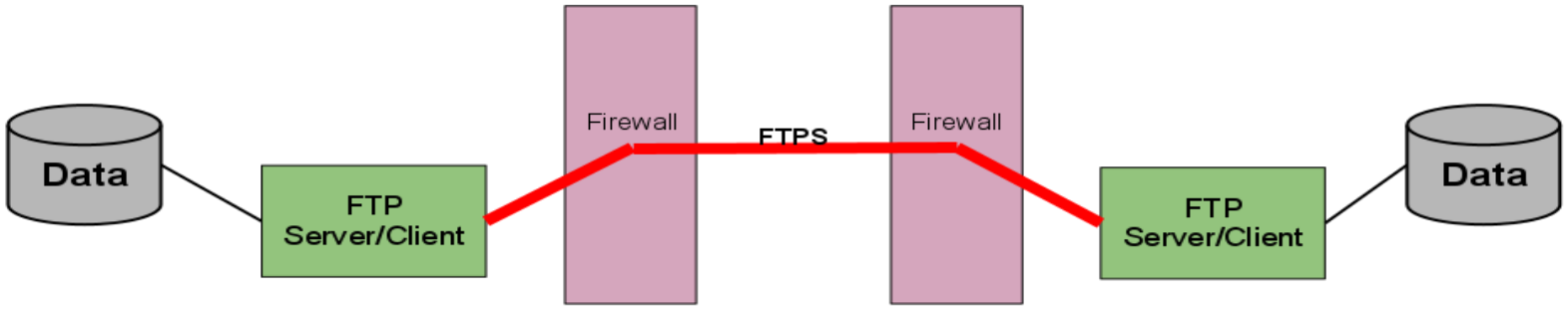


- Pros
  - Same FTP familiarity
  - Included in base z/OS
  - Supports X.509 certificates (trusted authority) and keberos
  - RACF keyrings supported
- Cons
  - Not firewall friendly (even worse than straight FTP)

Passive FTP

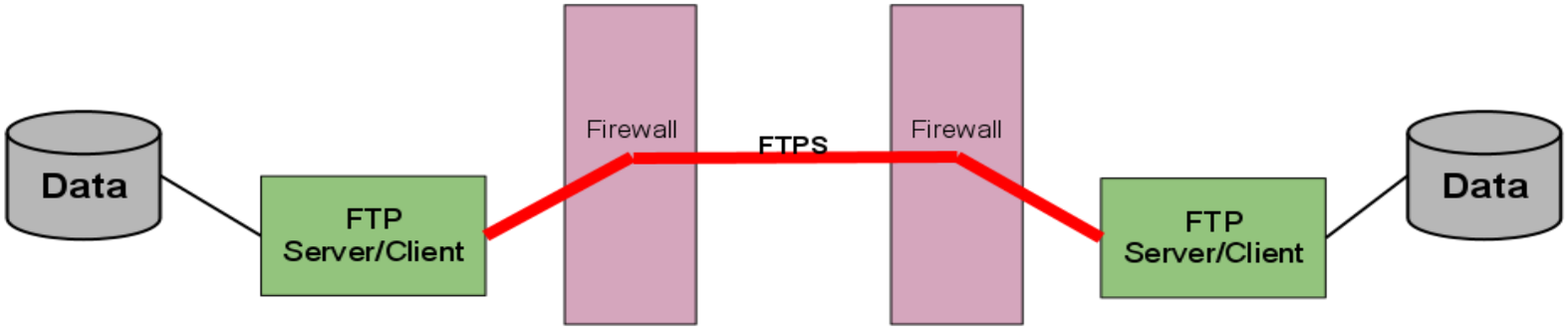


FTP over SSL (FTPS)



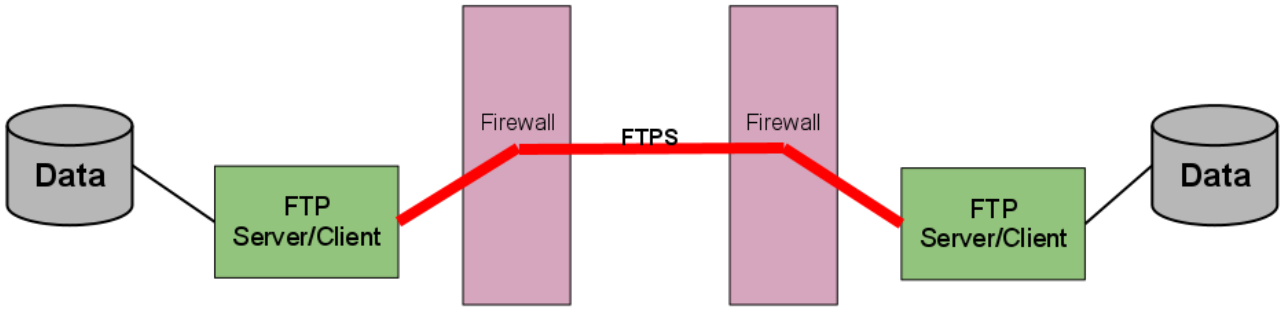
- Pros
  - Same FTP familiarity
  - Included in base z/OS
  - Supports X.509 certificates (trusted authority) and keberos
  - RACF keyrings supported
- Cons
  - Not firewall friendly (even worse than straight FTP)
  - Can't assume it's available on the other end

FTP over SSL (FTPS)



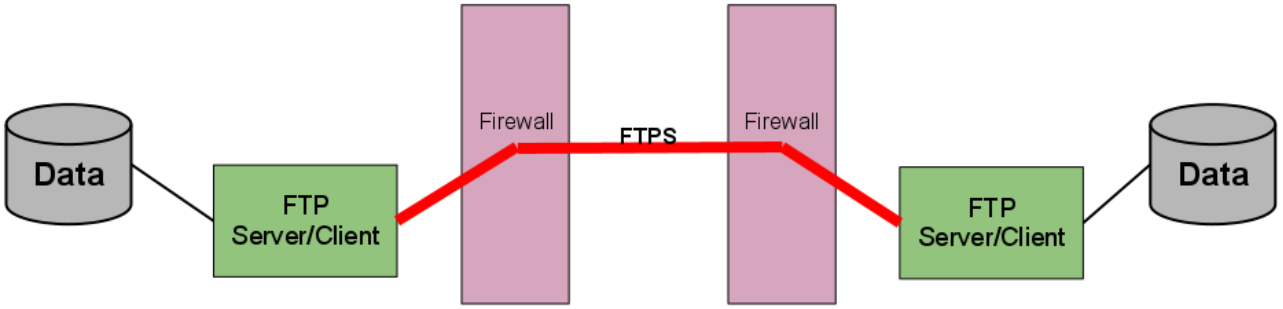
- Common Uses
  - z/OS to z/OS

FTP over SSL (FTPS)



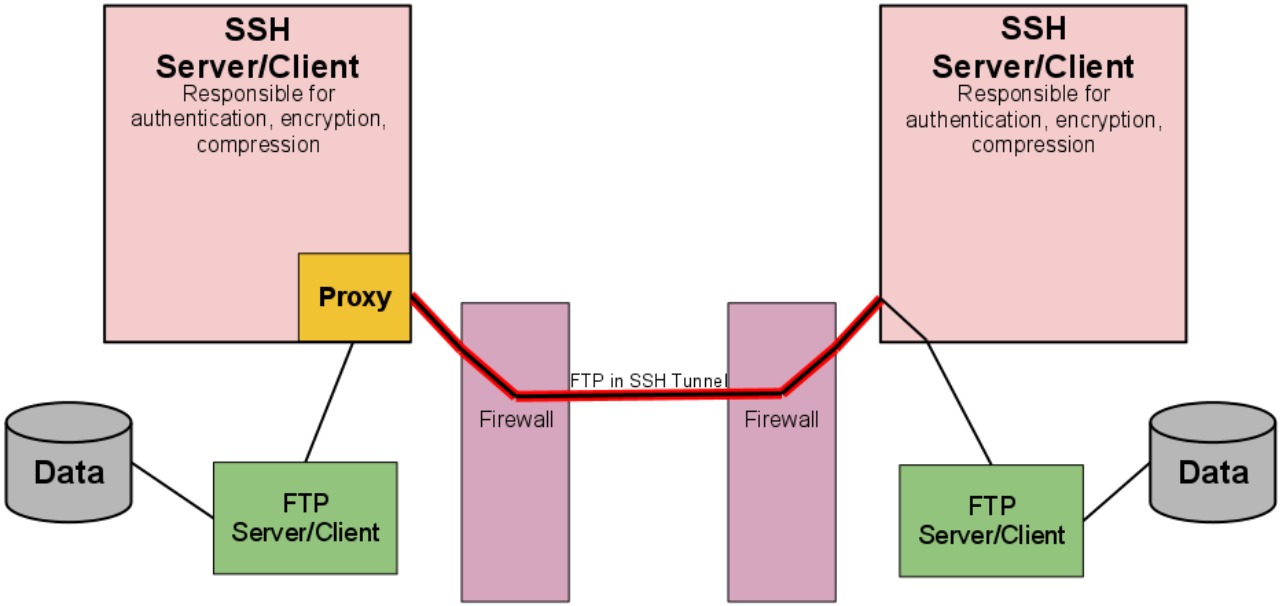
- Common Uses
  - z/OS to z/OS
  - z/OS to i/Series

FTP over SSL (FTPS)



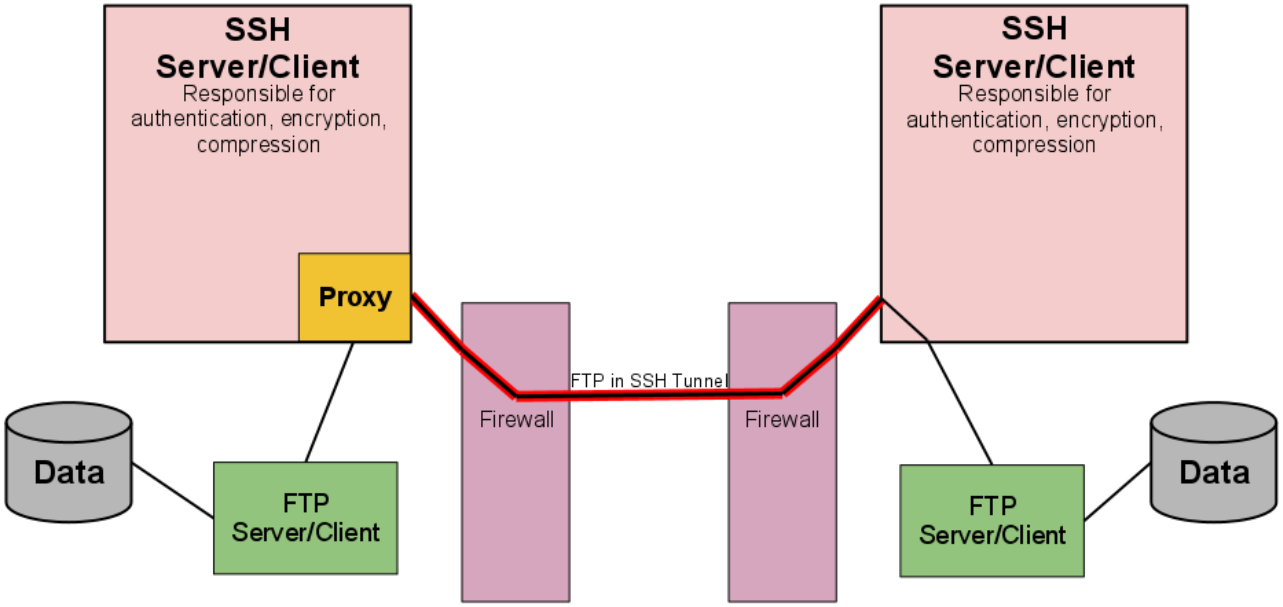
- Common Uses
  - z/OS to z/OS
  - z/OS to i/Series
  - Servers and clients available on platforms

FTP over SSH Tunnel



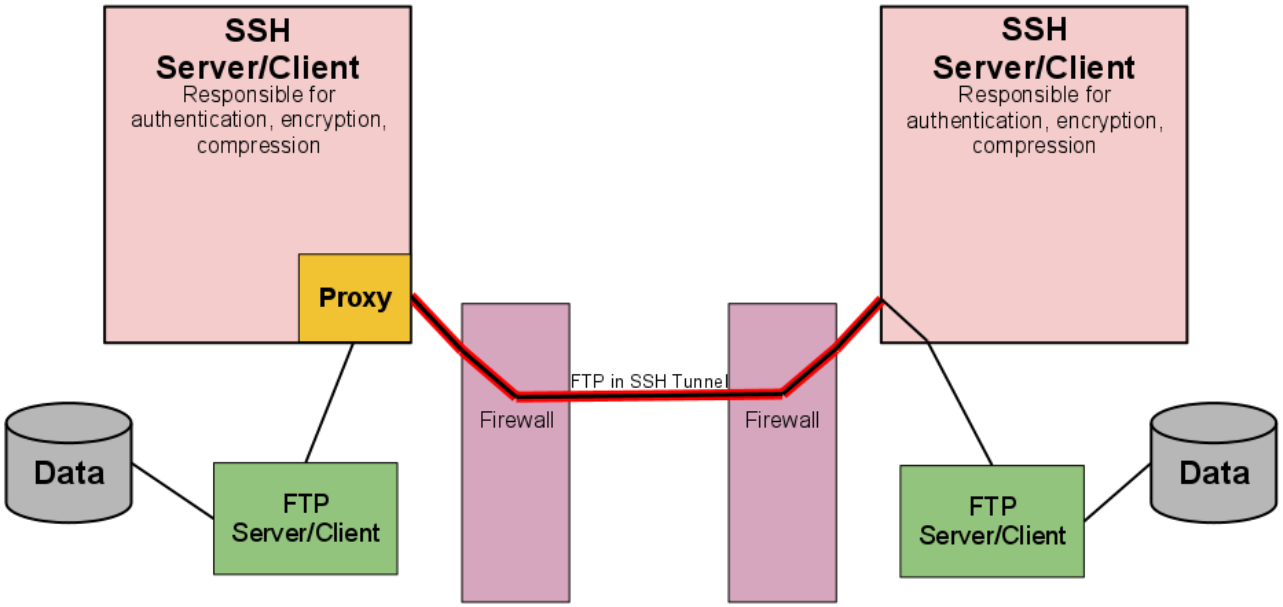
- Pros
  - Same FTP familiarity

FTP over SSH Tunnel



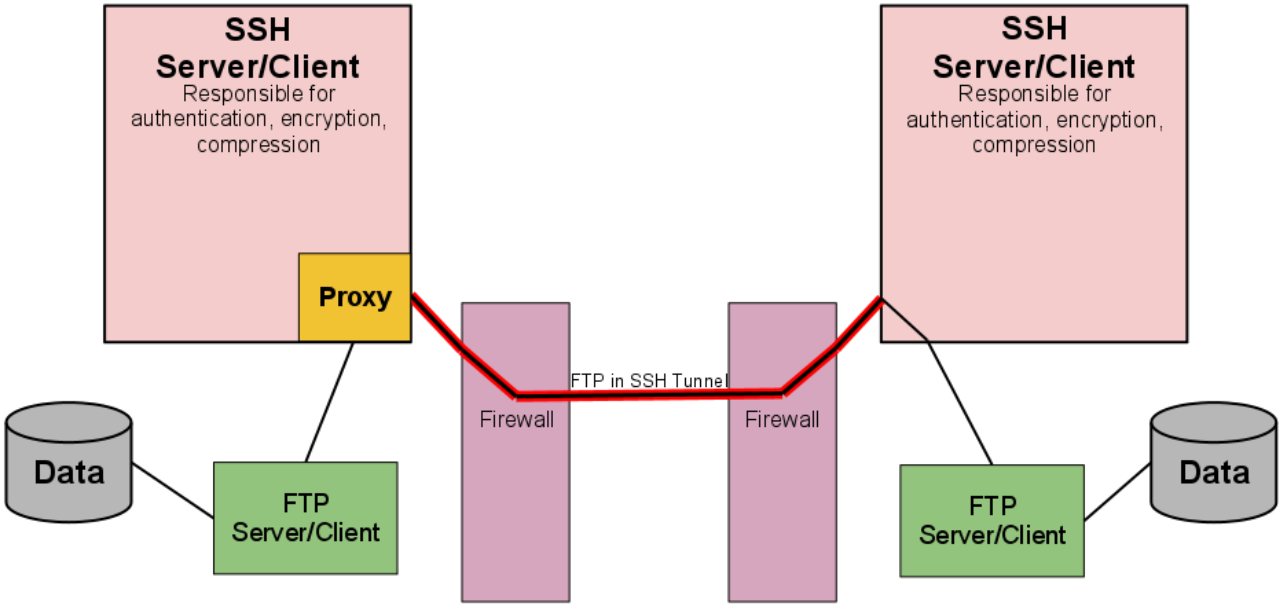
- Pros
  - Same FTP familiarity
  - Firewall friendly

FTP over SSH Tunnel



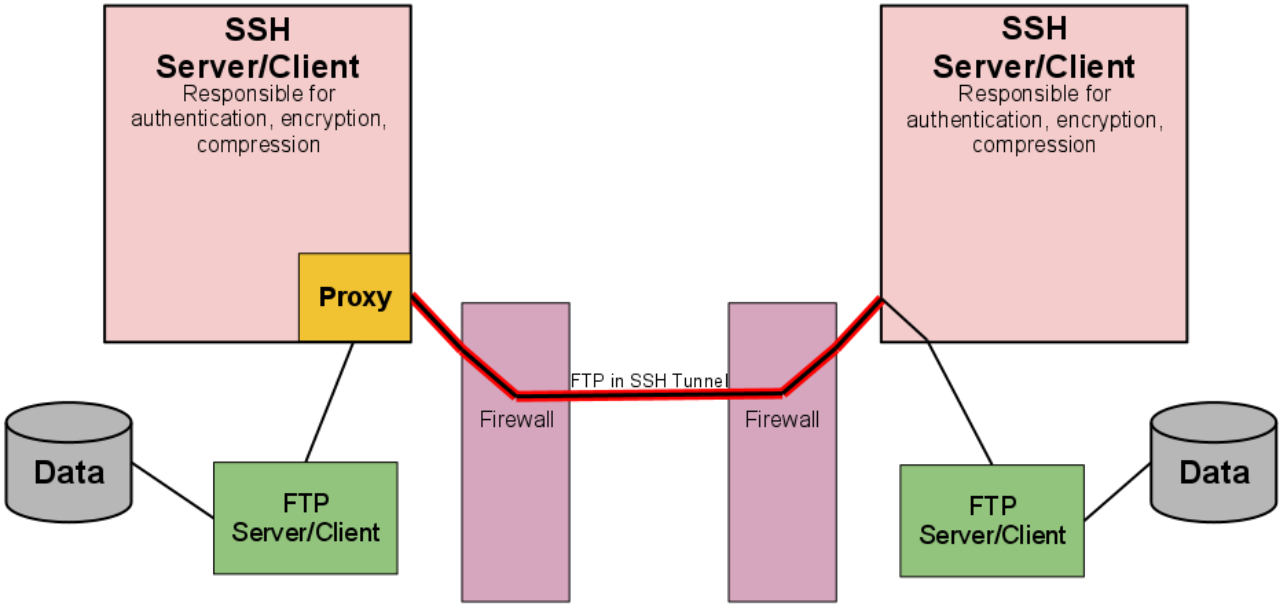
- Pros
  - Same FTP familiarity
  - Firewall friendly
  - Compression of data

FTP over SSH Tunnel



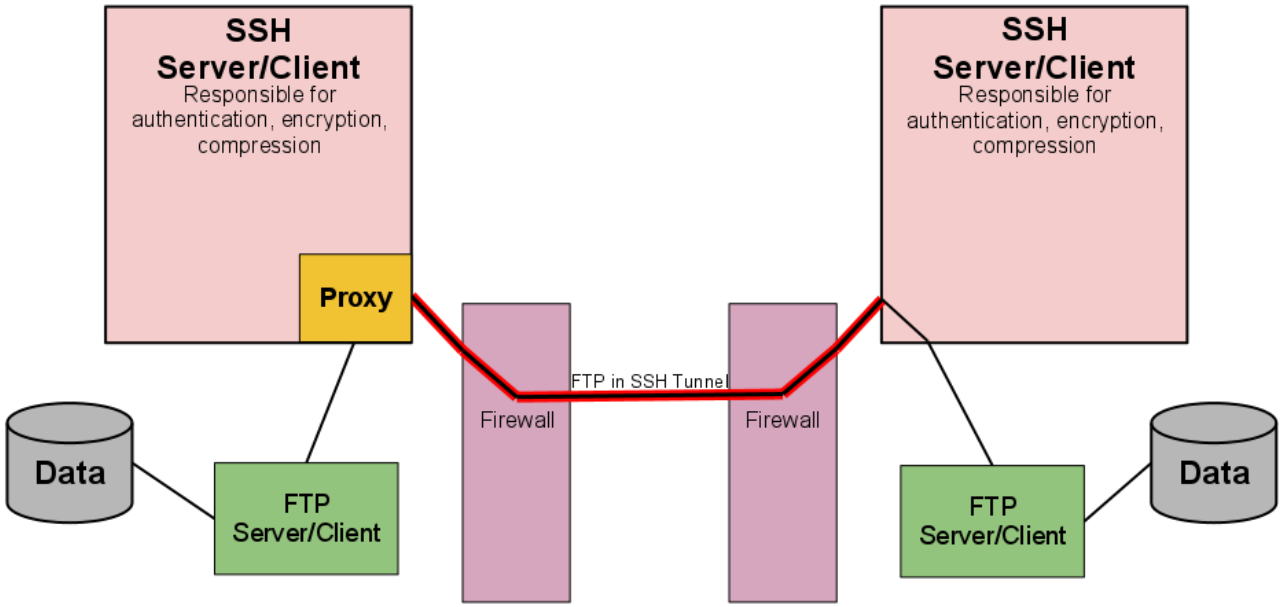
- Pros
  - Same FTP familiarity
  - Firewall friendly
  - Compression of data
  - Good checksums of data, at least for the internet piece

FTP over SSH Tunnel



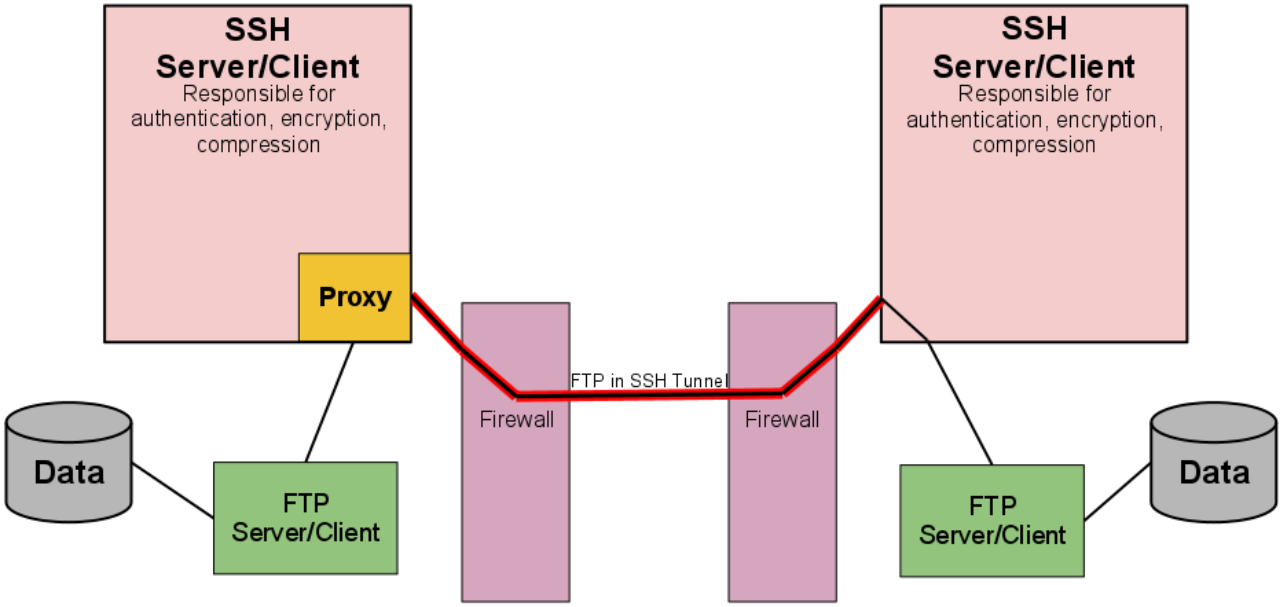
- Pros
  - Same FTP familiarity
  - Firewall friendly
  - Compression of data
  - Good checksums of data, at least for the internet piece
- Cons
  - More parts need to be choreographed

FTP over SSH Tunnel



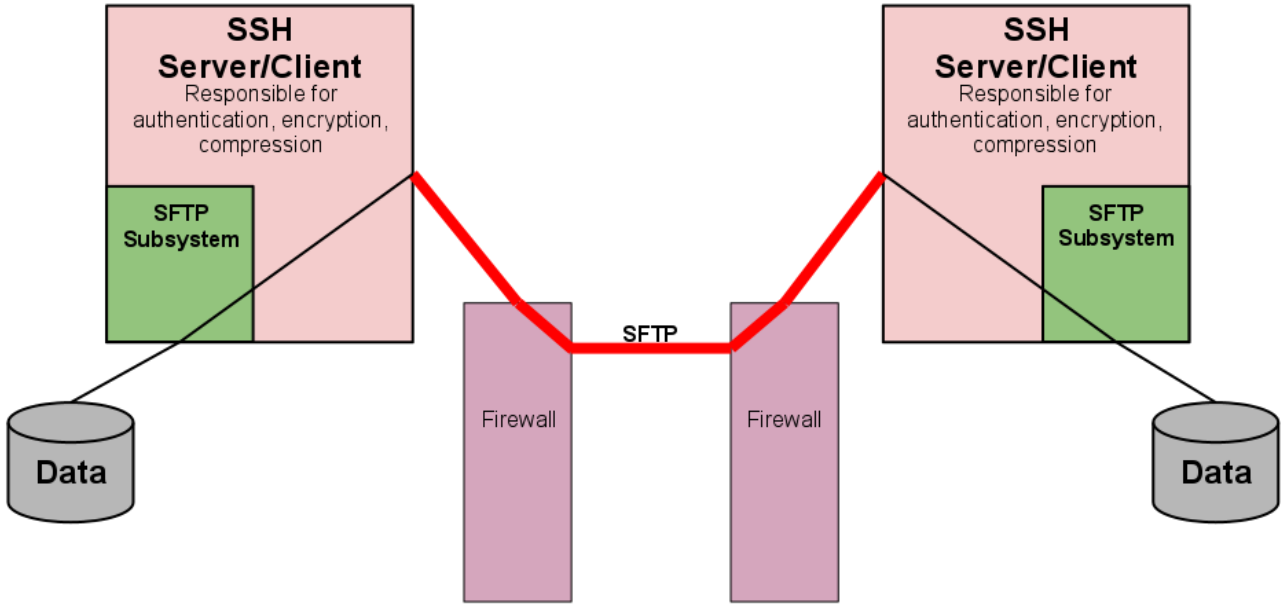
- Pros
  - Same FTP familiarity
  - Firewall friendly
  - Compression of data
  - Good checksums of data, at least for the internet piece
- Cons
  - More parts need to be choreographed
  - Requires SSH and FTP on both ends

FTP over SSH Tunnel



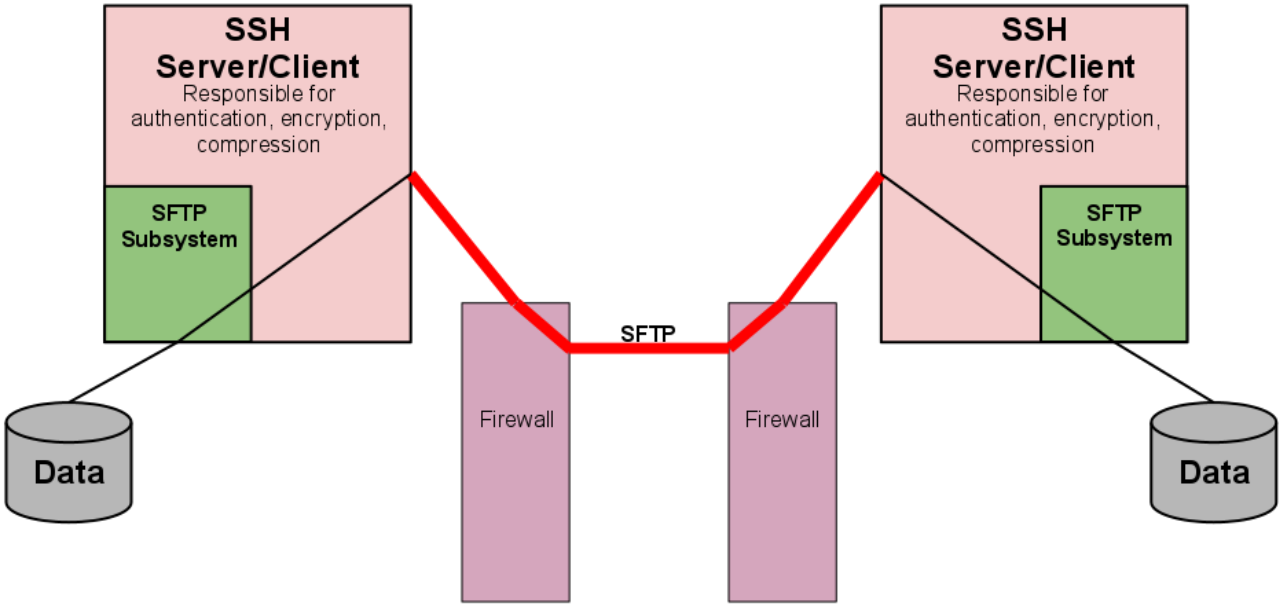
- Common uses
  - Sites that have a significant reliance on FTP already in place that need to implement SSH encryption for transit

Secure FTP (SFTP)



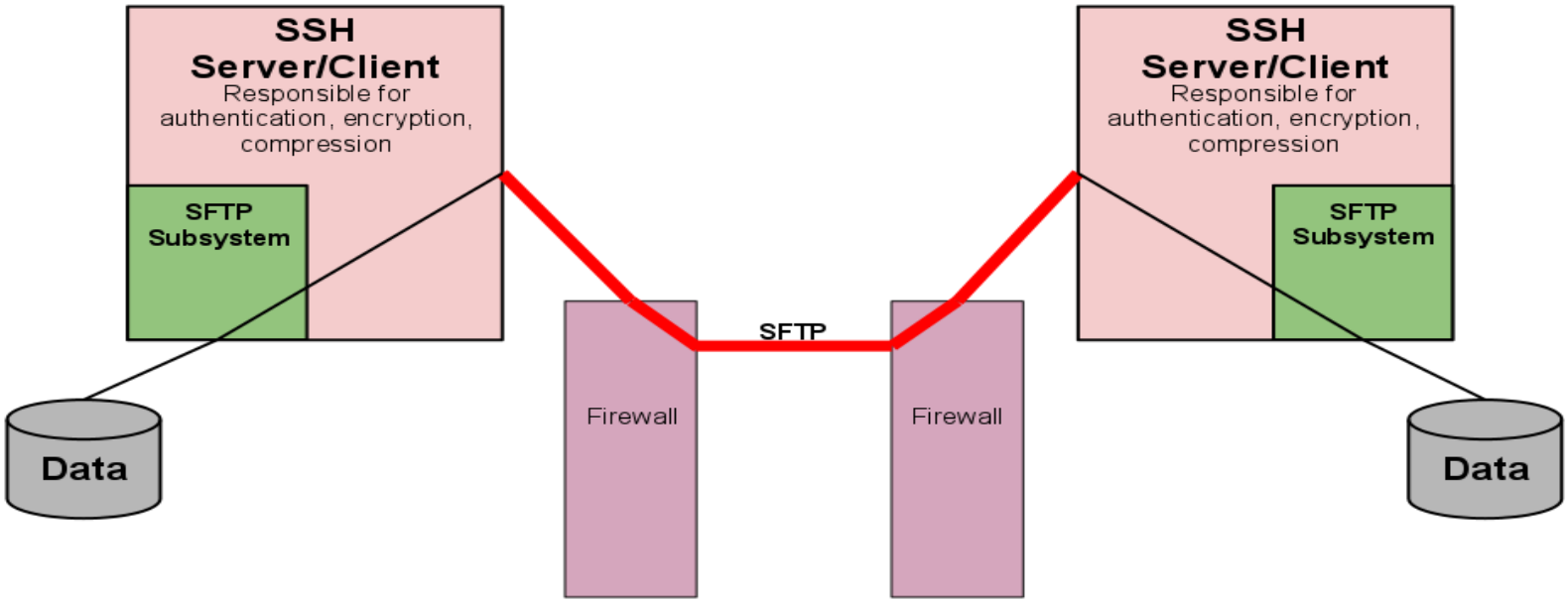
- Pros
  - Point to point encryption

Secure FTP (SFTP)



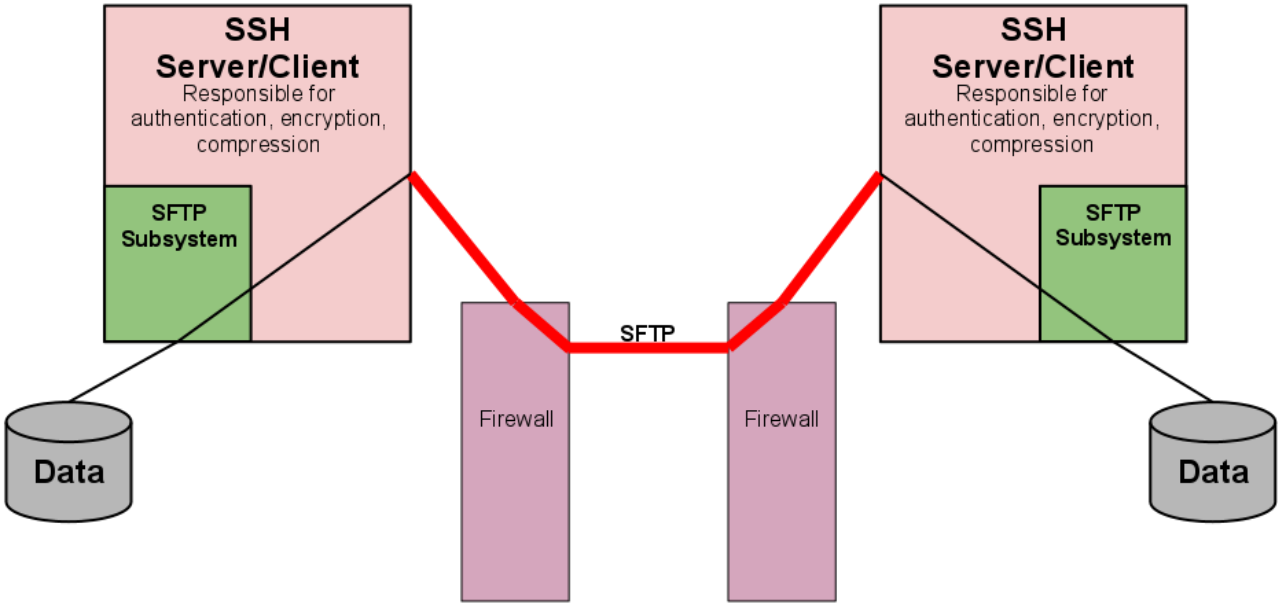
- Pros
  - Point to point encryption
  - Compression and Integrity built-in

Secure FTP (SFTP)



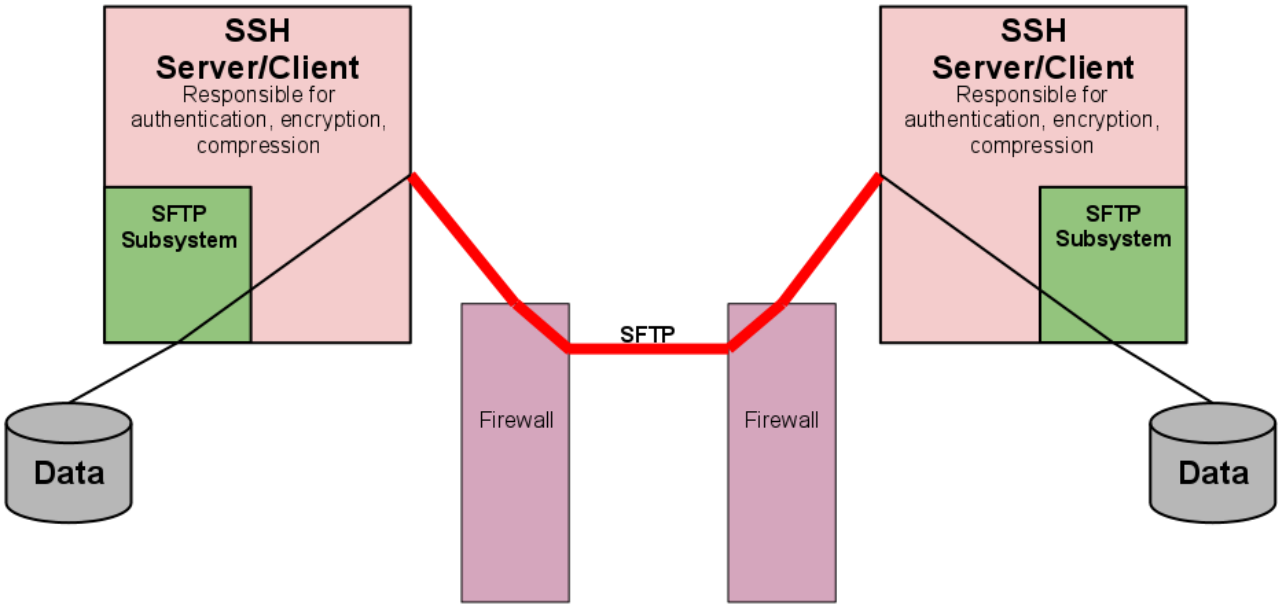
- Pros
  - Point to point encryption
  - Compression and Integrity built-in
  - Already ready to go on Unix/Linux servers

Secure FTP (SFTP)



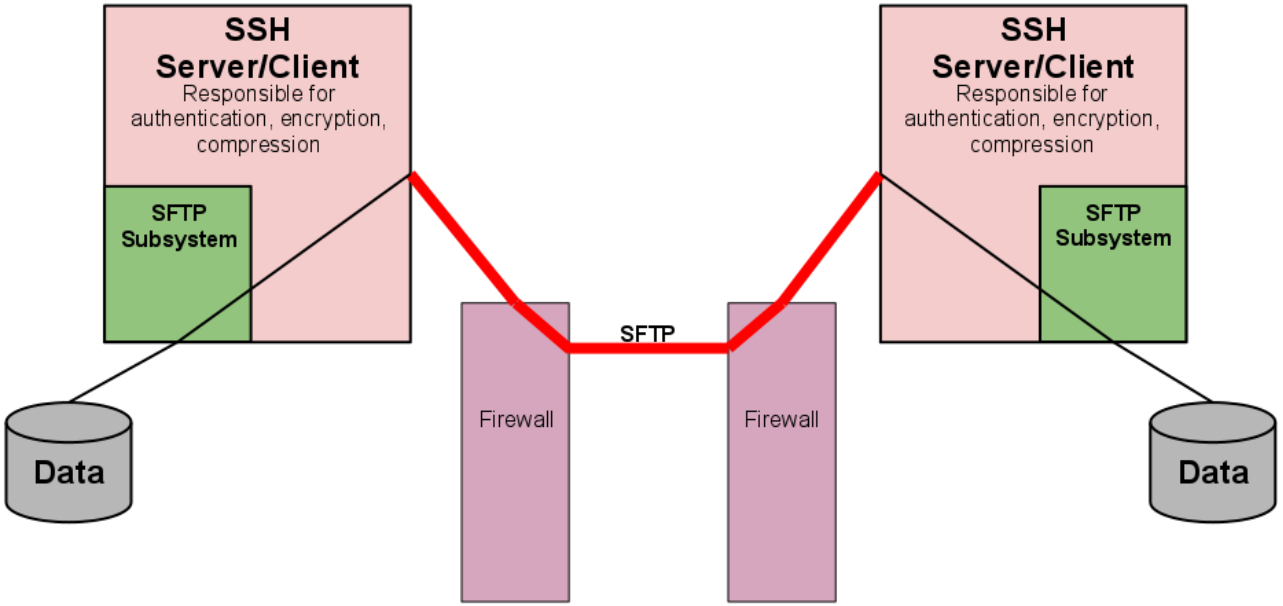
- Pros
  - Point to point encryption
  - Compression and Integrity built-in
  - Already ready to go on Unix/Linux servers
- Cons
  - Not part of base on z/OS or Windows

Secure FTP (SFTP)



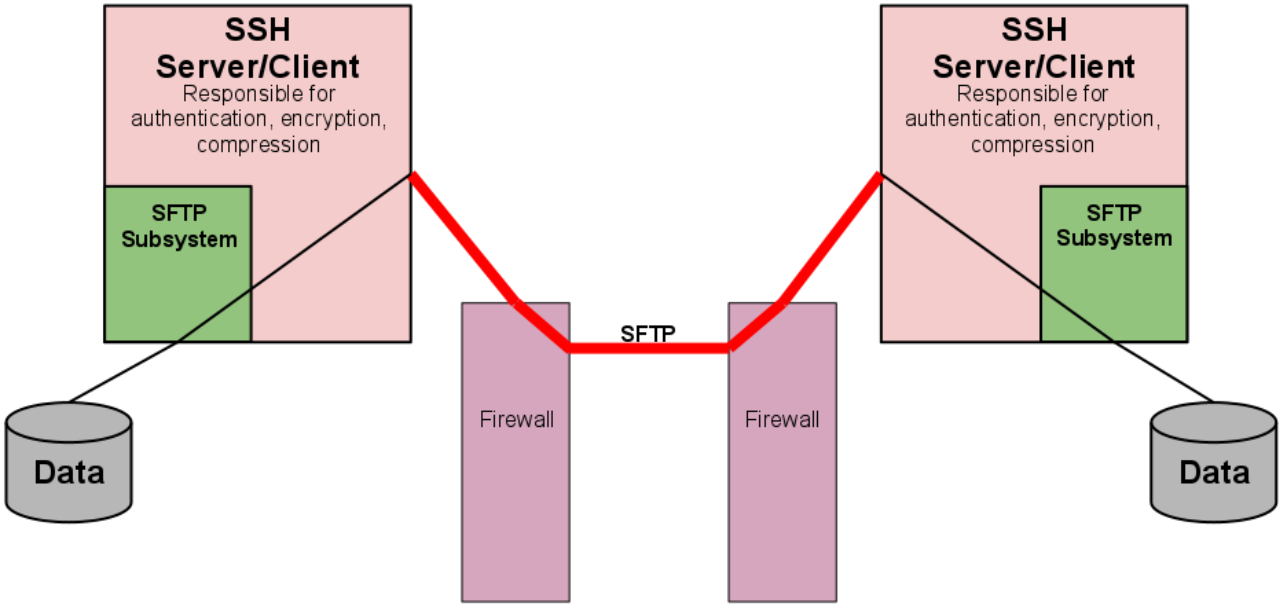
- Pros
  - Point to point encryption
  - Compression and Integrity built-in
  - Already ready to go on Unix/Linux servers
- Cons
  - Not part of base on z/OS or windows
  - May not be as familiar to users

Secure FTP (SFTP)



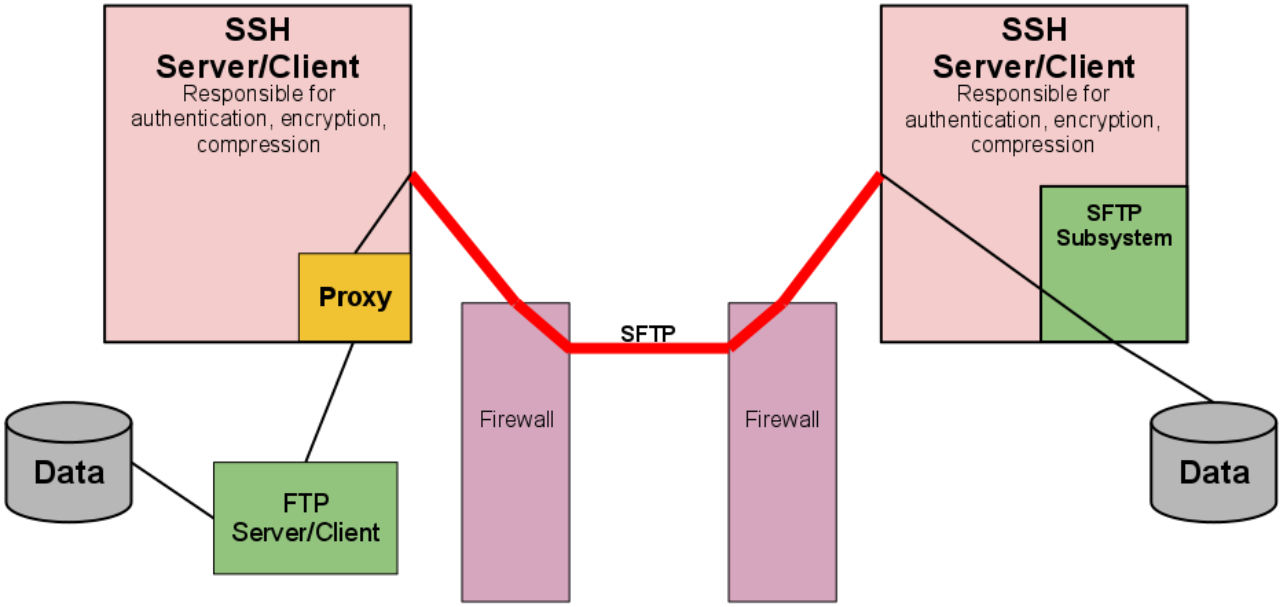
- Pros
  - Point to point encryption
  - Compression and Integrity built-in
  - Already ready to go on Unix/Linux servers
- Cons
  - Not part of base on z/OS or windows
  - May not be as familiar to users
  - Only protects data in transit

Secure FTP (SFTP)



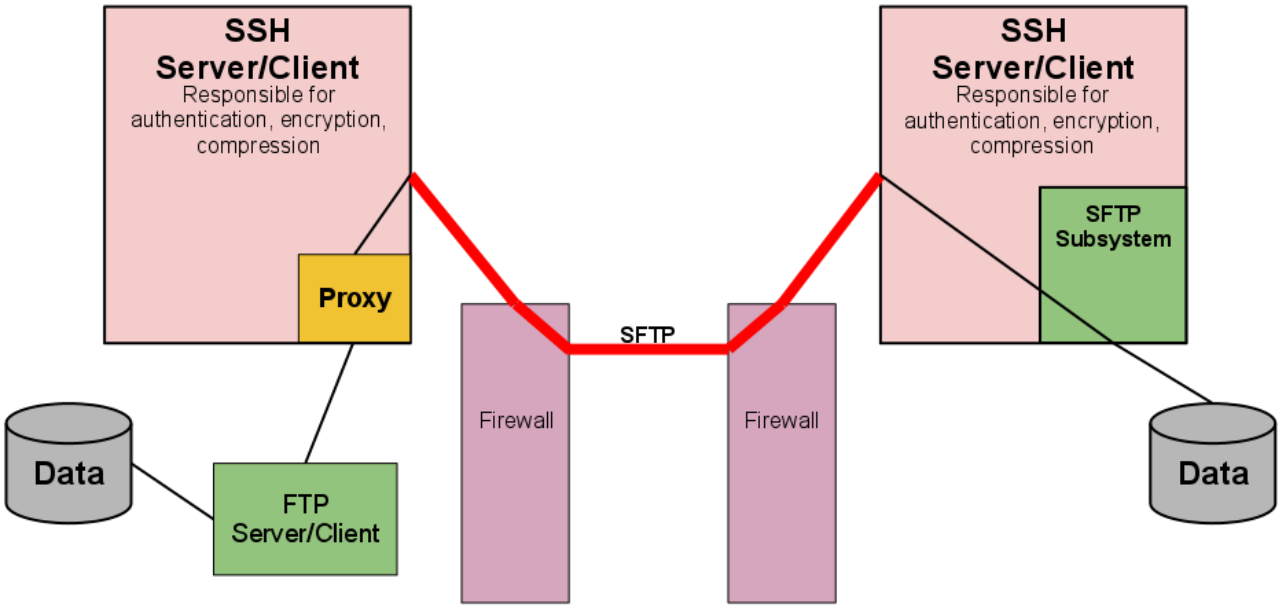
- Common uses
  - Easy access for distribution to Unix/Linux farms

FTP to SFTP Conversion (Vendor Solution)



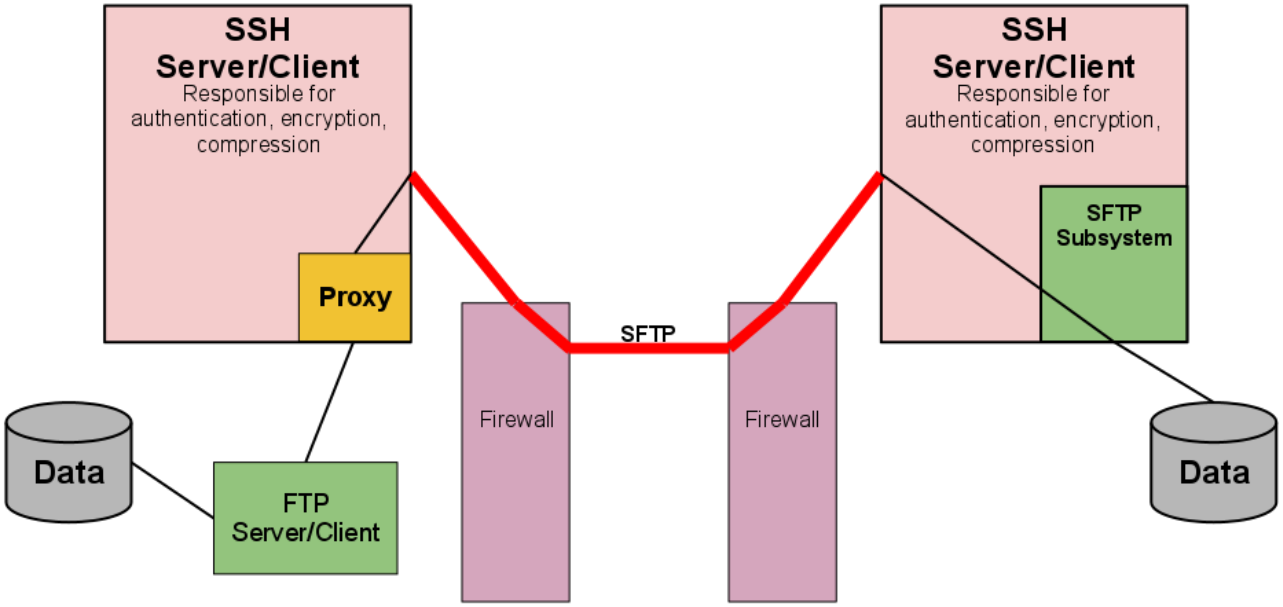
- Pros
  - Satisfies SFTP requirement

FTP to SFTP Conversion (Vendor Solution)



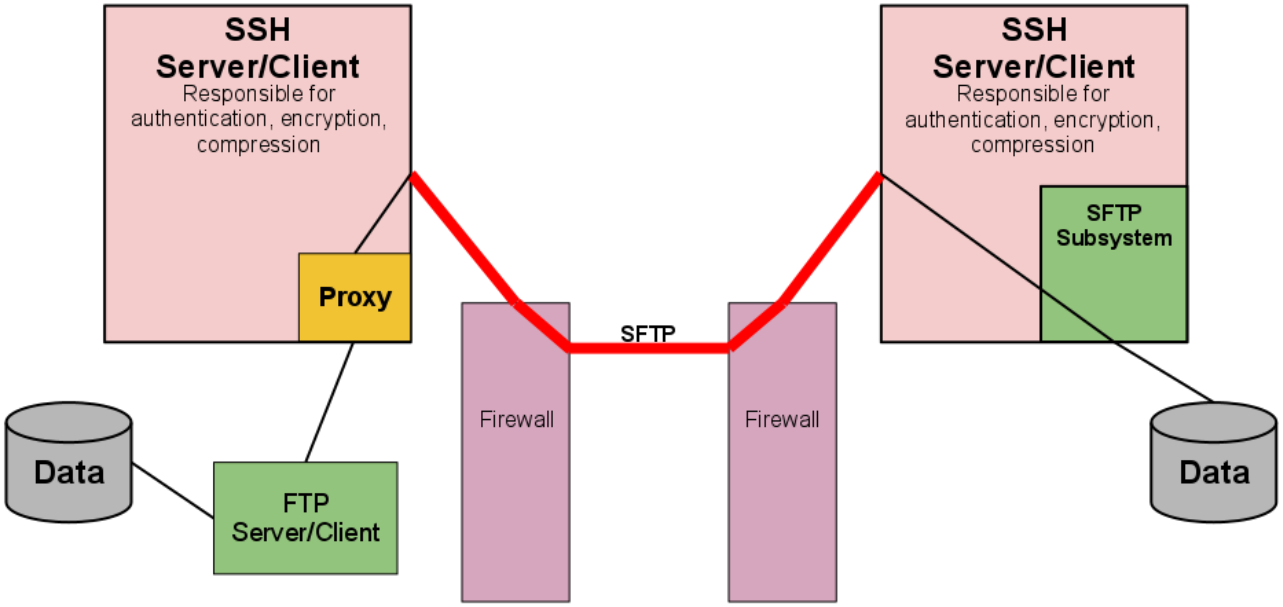
- Pros
  - Satisfies SFTP requirement
  - Can still use the FTP client on the z/OS side

FTP to SFTP Conversion (Vendor Solution)



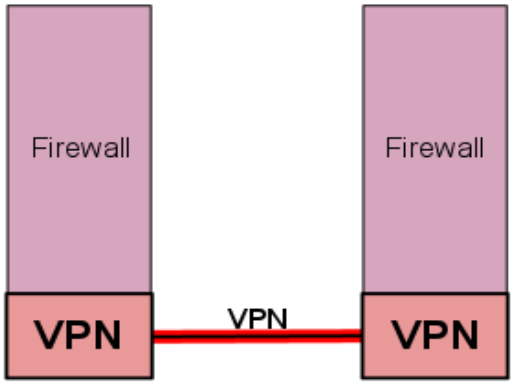
- Pros
  - Satisfies SFTP requirement
  - Can still use the FTP client on the z/OS side
- Cons
  - Not a perfect match of functions

FTP to SFTP Conversion (Vendor Solution)



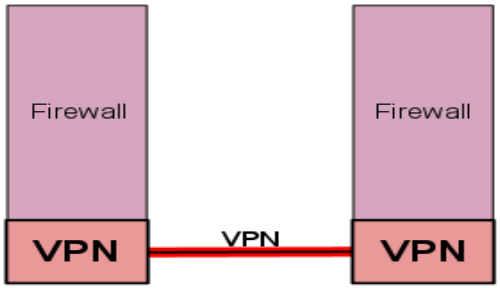
- Common uses
  - Leveraging FTP already in place, but transitioning it to your SFTP knowledgeable partners

VPN



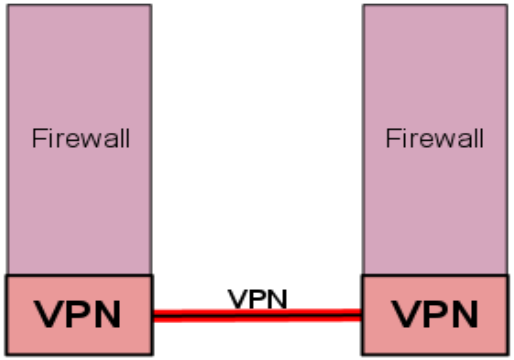
- Pros
  - Network to Network encryption (everything covered)

VPN



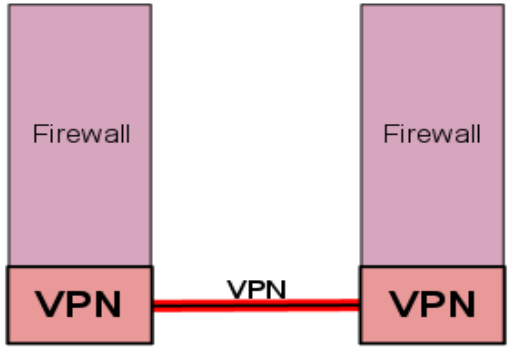
- Pros
  - Network to Network encryption (everything covered)
  - Some integrity built-in

VPN



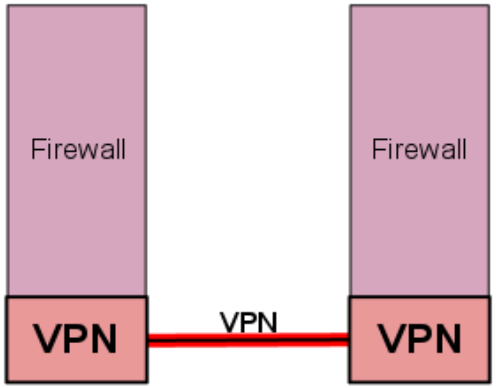
- Pros
  - Network to Network encryption (everything covered)
  - Some integrity built-in
  - Compression might be included

VPN



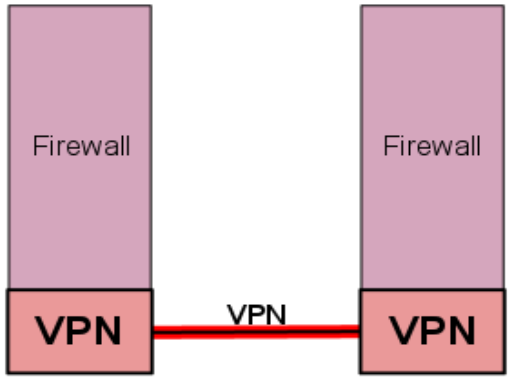
- Pros
  - Network to Network encryption (everything covered)
  - Some integrity built-in
  - Compression might be included
  - Transparent to the applications

VPN



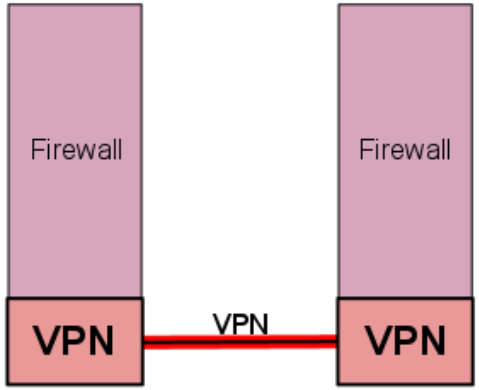
- Pros
  - Network to Network encryption (everything covered)
  - Some integrity built-in
  - Compression might be included
  - Transparent to the applications
- Cons
  - More complex to set up

VPN



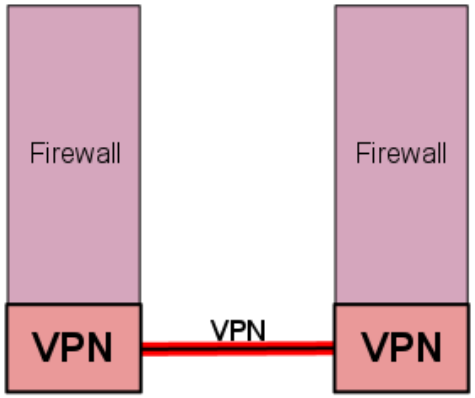
- Pros
  - Network to Network encryption (everything covered)
  - Some integrity built-in
  - Compression might be included
  - Transparent to the applications
- Cons
  - More complex to set up
  - Intranet traffic is unprotected

VPN



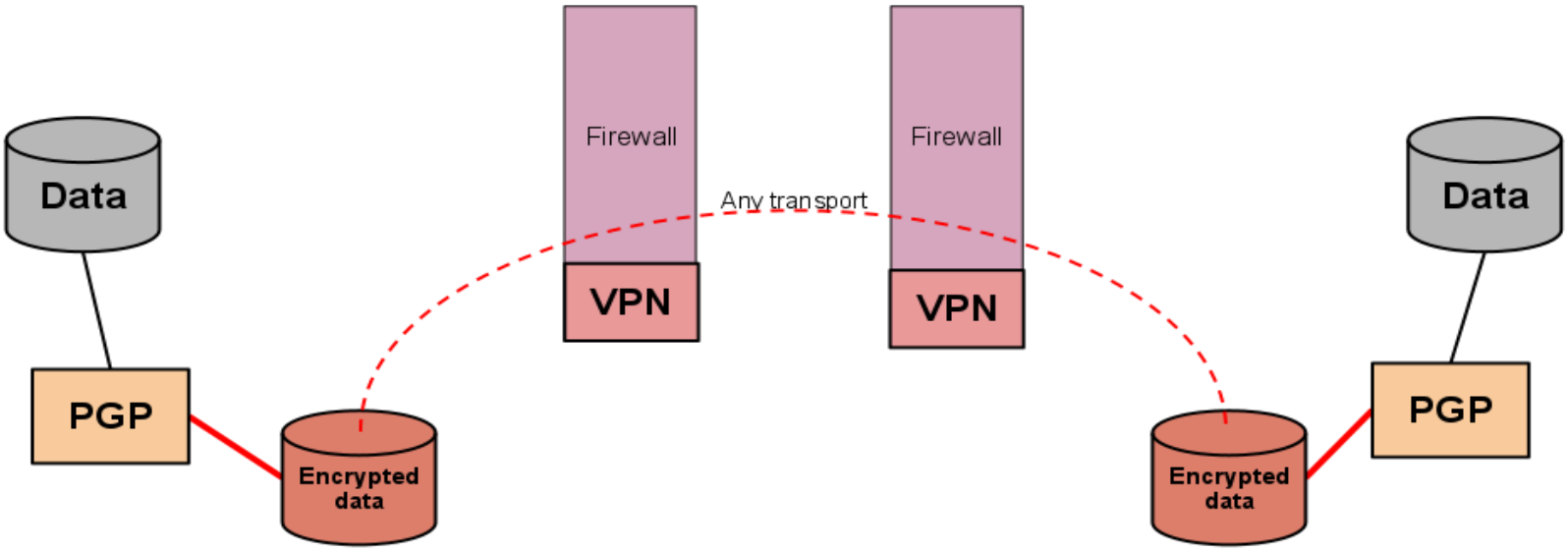
- Pros
  - Network to Network encryption (everything covered)
  - Some integrity built-in
  - Compression might be included
  - Transparent to the applications
- Cons
  - More complex to set up
  - Intranet traffic is unprotected
  - Usually managed by another group

VPN



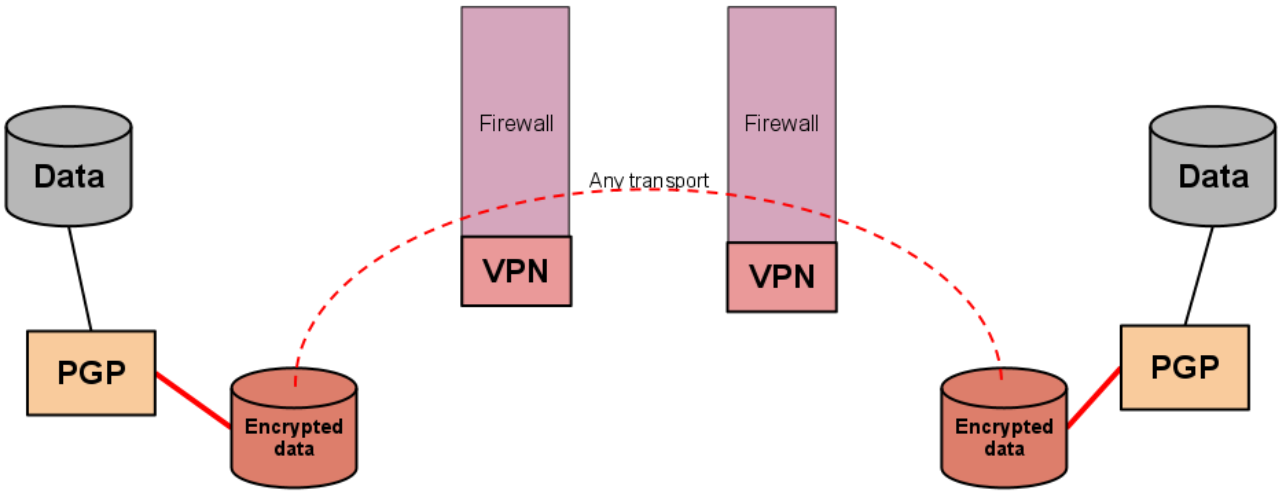
- Common uses
  - Trusted partner networks

PGP (Data at Rest)



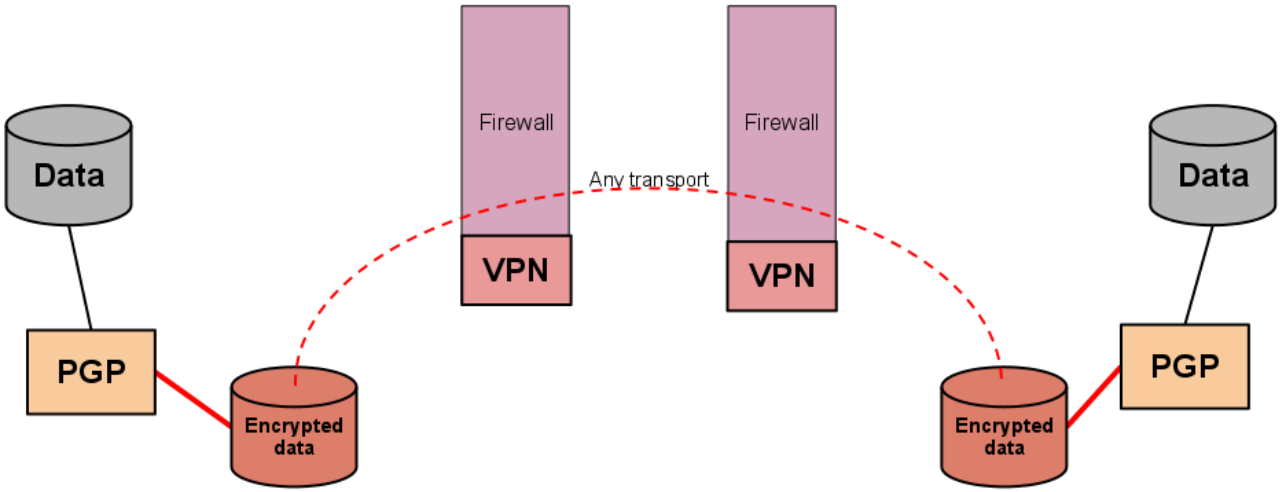
- Pros
  - Full control of sensitive data

PGP (Data at Rest)



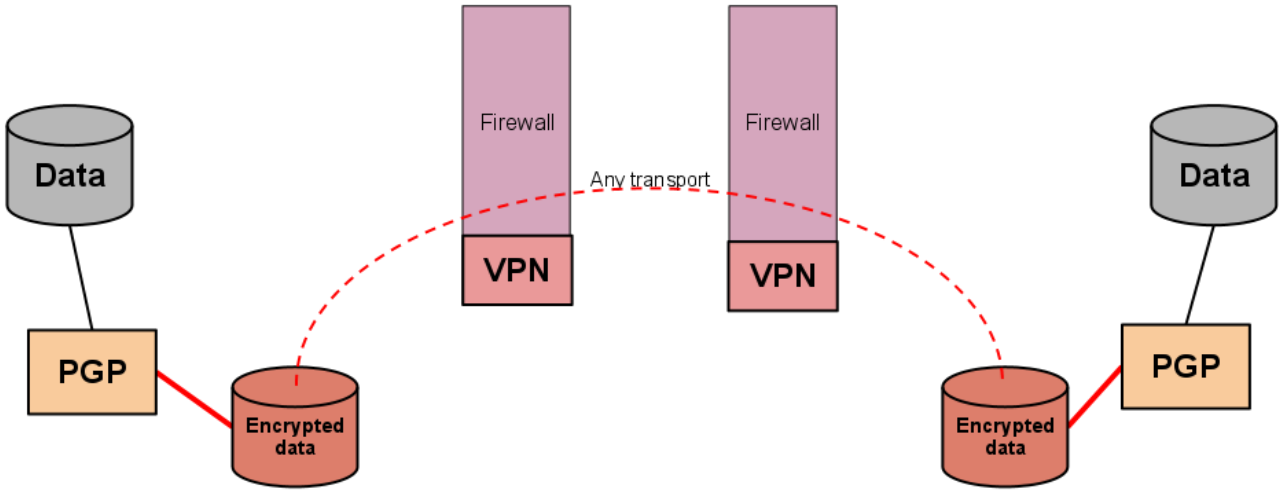
- Pros
  - Full control of sensitive data
  - Transport is not important

PGP (Data at Rest)



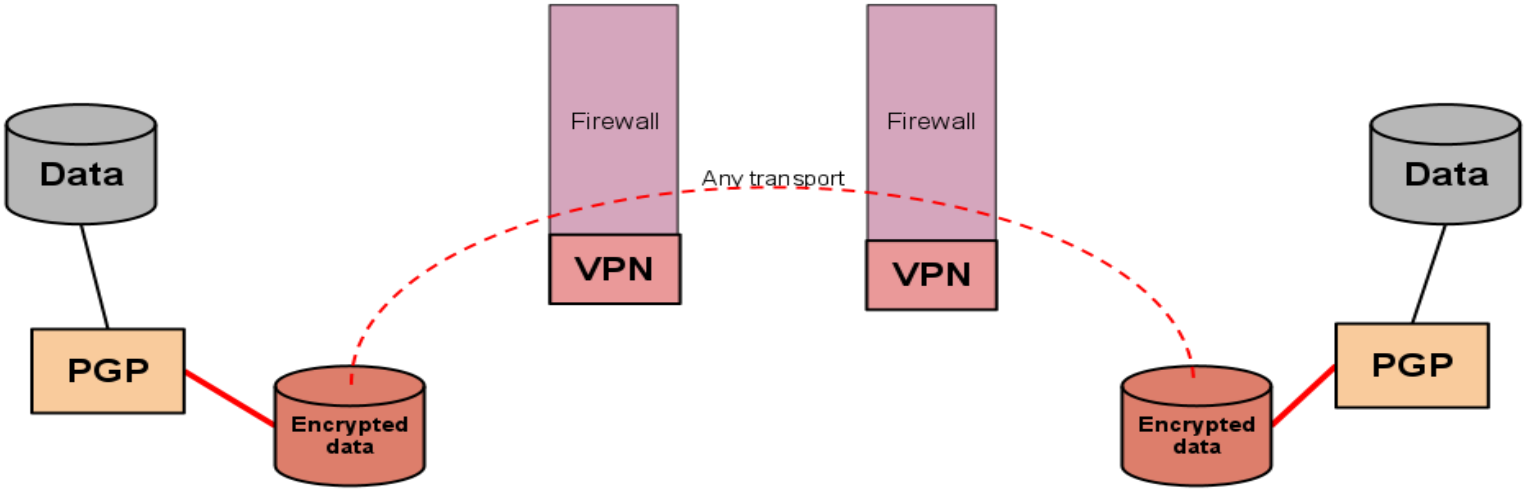
- Pros
  - Full control of sensitive data
  - Transport is not important
  - Compression and Integrity

PGP (Data at Rest)



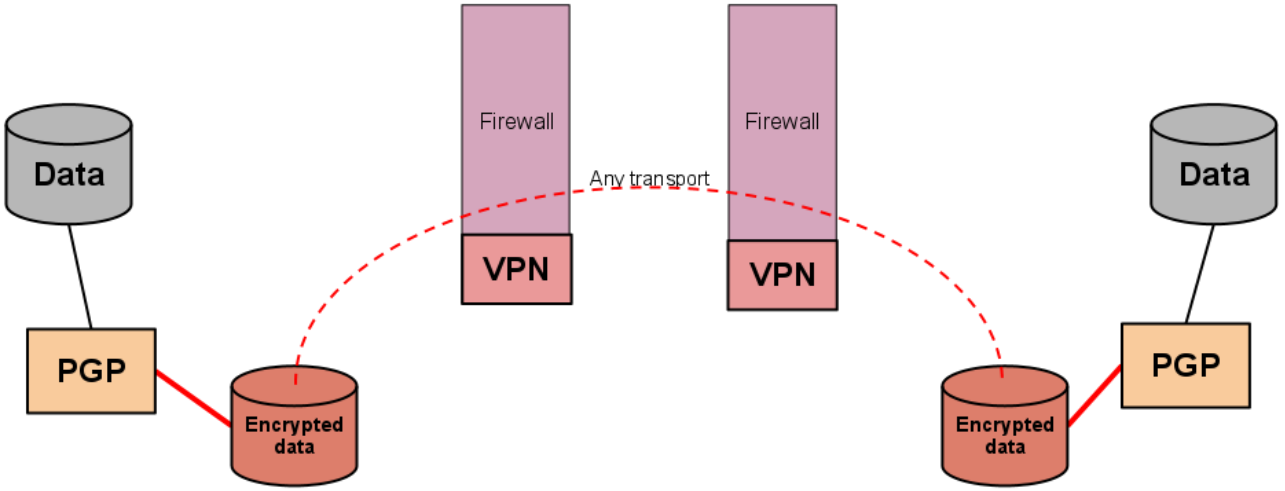
- Pros
  - Full control of sensitive data
  - Transport is not important
  - Compression and Integrity
  - Not just for transfers

PGP (Data at Rest)



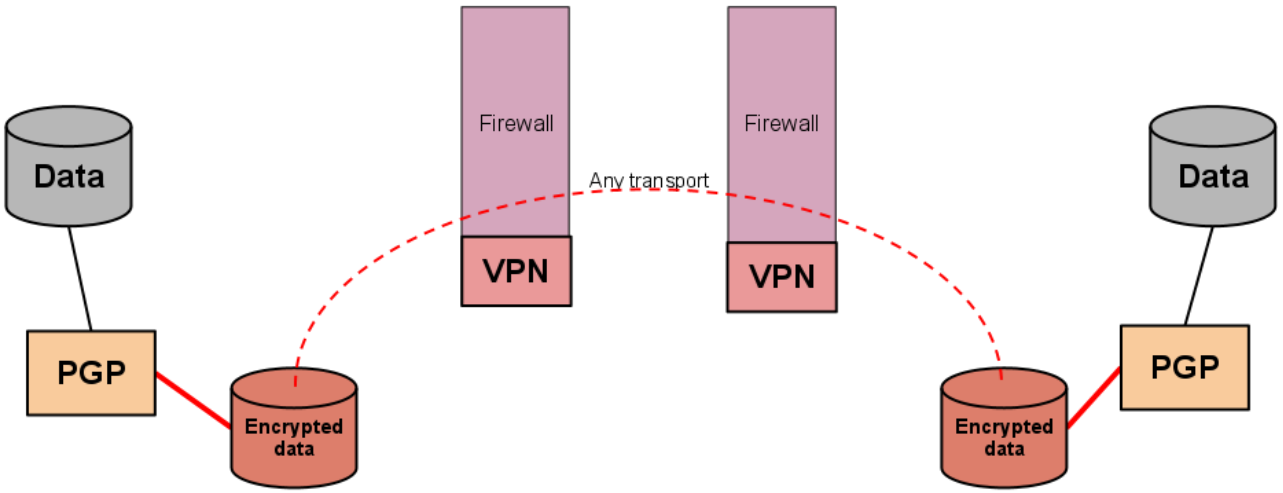
- Pros
  - Full control of sensitive data
  - Transport is not important
  - Compression and Integrity
  - Not just for transfers
- Cons
  - Requires staging of data

PGP (Data at Rest)



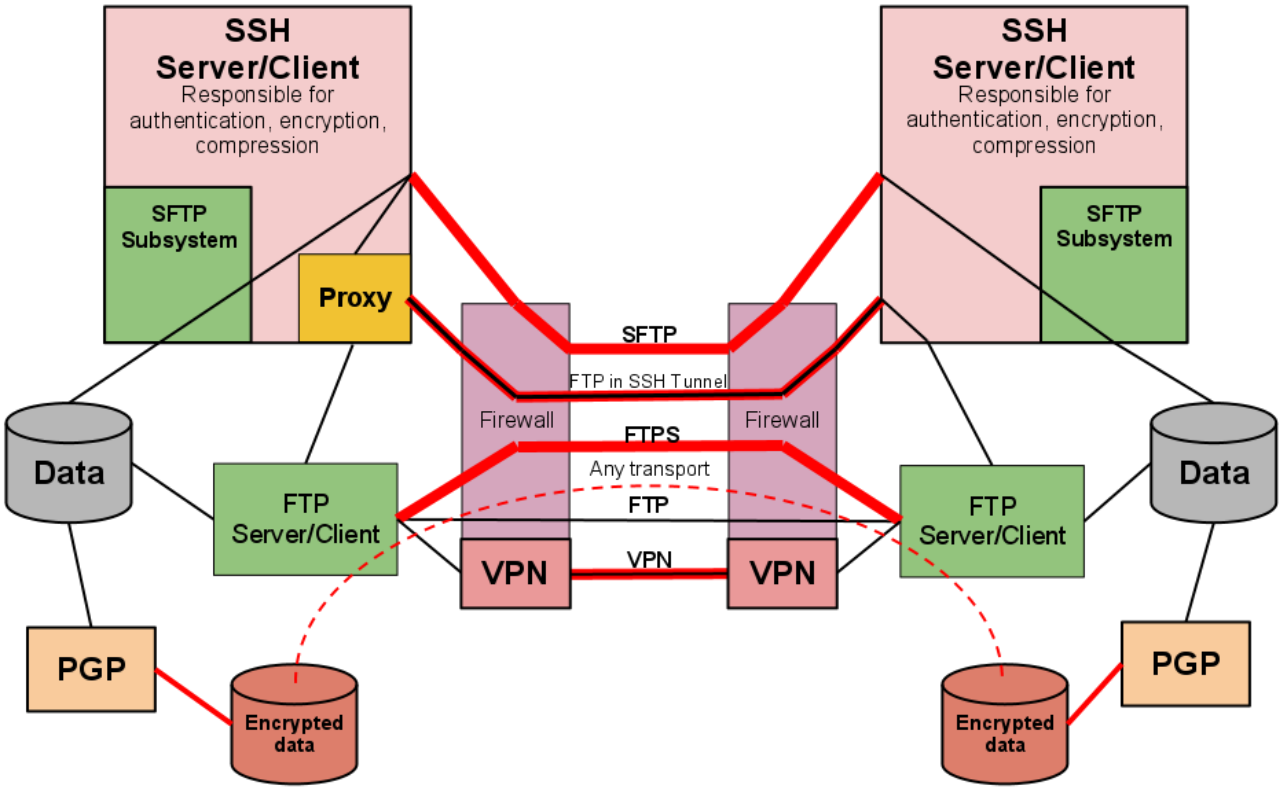
- Common uses
  - Sensitive data that needs protection at destination as well as in transit

PGP (Data at Rest)



- Common uses
  - Sensitive data that needs protection at destination as well as in transit
  - When network component is not managed by interested parties

FTP – All The Options



- Common uses
  - Mixed requirements – unfortunately, one size rarely fits all properly

Thank You