

CAIL Security Facility



CAIL

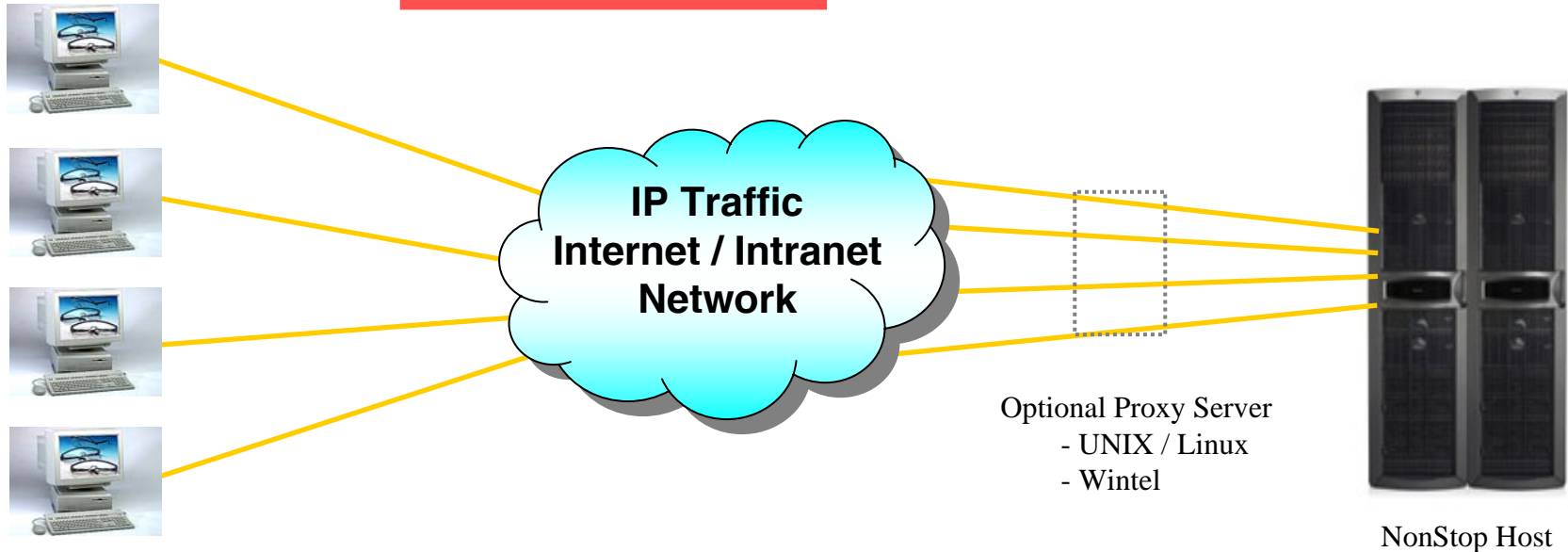
CAIL Security Facility

Table of Contents

- A. Overview**
- B. CAIL Security Solutions**
- C. Summary**

CAIL Security Facility

A1. Overview



Windows / Browser

1. Client

- Windows
 - Traditional
 - ActiveX
- Browser
 - Java
 - ActiveX
 - HTML

2. Communications

- Encryption options
- SSL
- DES 56, 168 bit
- AES
- D/H Key Exchange
- SSH
- SFTP

3. Proxy Server

Optional Unix / Linux or Windows System run Java based applications to augment Guardian based NonStop Host applications for secure communications.
(See Section B3)

4. NonStop Host

The CAIL Security Facility resides on a NonStop or an external Proxy Server. CAIL supports both Guardian and OSS based systems.
(See Section B4 & B5)

CAIL Security Facility

A2. Overview

The CAIL Security Facility includes software that resides on a NonStop server to extend your connectivity and security capabilities. The components are:

Function:	Security Manger	Audit	Application Protocol - FTP - Telnet - ODBC - RSC - etc.	Smart Adapters	Comm. Protocols - TCP/IP - Asynch - Multilan - SPX/IPX
Host:	•Guardian/NSK •Unix/OSS •Wintel	•Guardian/NSK •Unix/OSS •Wintel	•Guardian /NSK •Unix/OSS •Wintel	• --- •Unix/OSS • ---	•Guardian/NSK •--- • ---

- Comments:**
- each of the above “Functions” of the CAIL Security Facility can be used with any of the Host platforms indicated.
 - Host based “CAIL Functions” are transparent to the applications and systems infrastructure.
 - the CAIL Security Facility - is included in CAIL/Suite
 - can be used with CAIL and non-CAIL clients

CAIL Security Facility

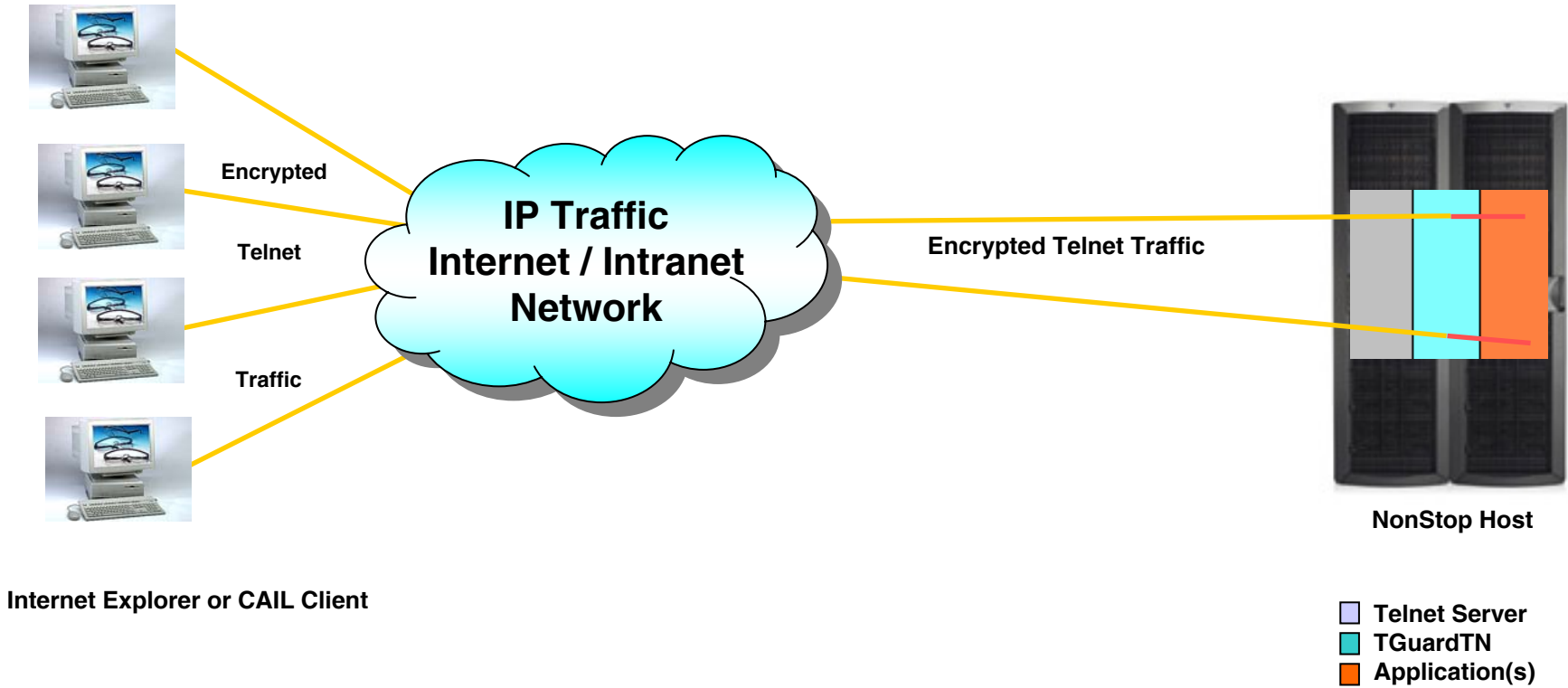
B. CAIL Security Solutions

You have the ability with CAIL to easily, quickly and at no extra cost improve system security as follows :

1. **TGuardTN – True Telnet End-to-End Encryption**
2. **TGuardALL – Host Resident Proxy Security
– Middleware Encryption (ODBC, RSC, etc.)**
3. **TGuardSSL – SSL Host Resident Proxy Security**
4. **TGuardFTP – FTP Host Resident Proxy Security**
5. **JGuardSSL – Front end Proxy using Java or OSS based
Host Proxy**
6. **JGuardFTP – Java SSL FTP Proxy Security**
7. **SSH / SFTP Client for UNIX**
8. **CAIL XML Adapter HTTPS**

CAIL Security Facility

B1. TGuardTN: True End-to-End Encryption



Communications Legend: — secure (encrypted) — “ clear “



CAIL Security Facility

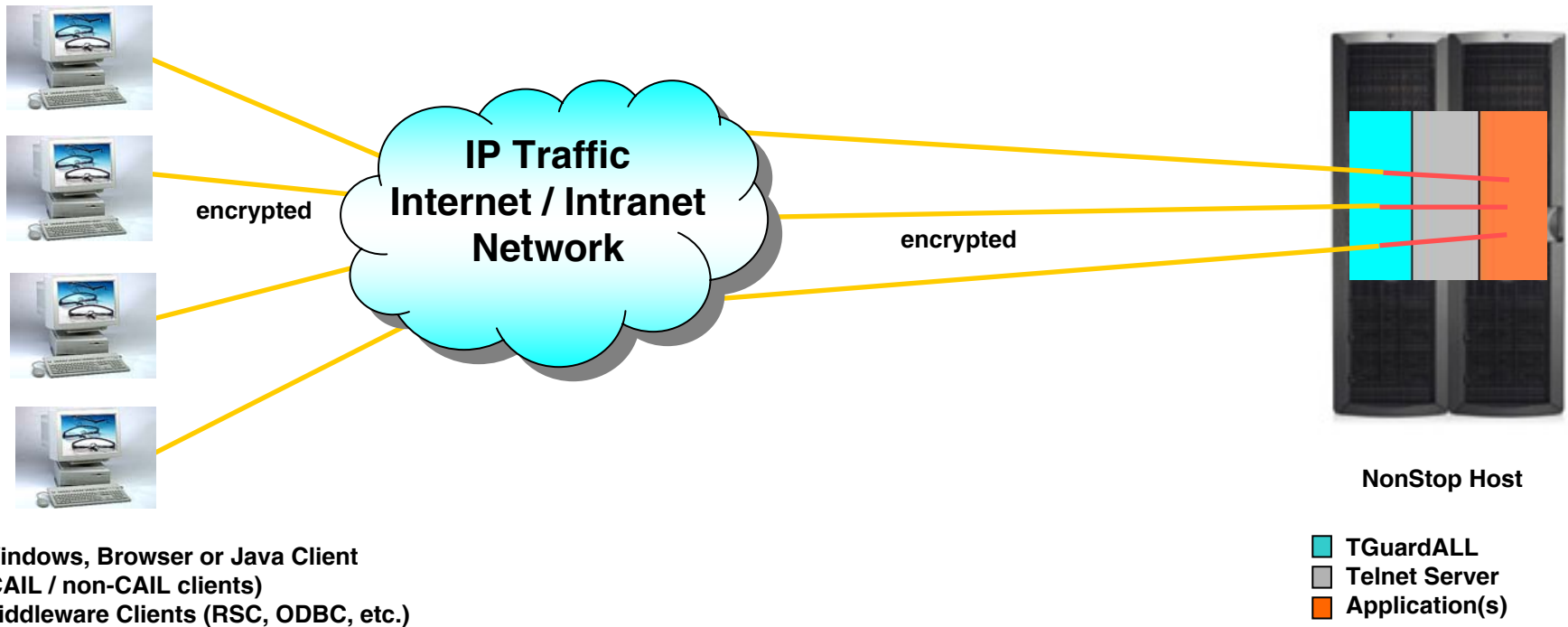
B1. TGuardTN: True End-to-End Encryption

Highlights:

- “True End-To-End Encryption” – While other NonStop implementations provide clear text to the NonStop Telnet server, TGuardTN keeps all traffic through the Telnet Server encrypted. The application is the only process that sees clear text.
- Works with all NonStop 6530 access methods - TGuardTN was designed to allow encryption to be used with all NonStop 6530 access methods including async, X.25, MultiLAN or any other NonStop access methods. NonStop terminal data does not go through IP networks exclusively. There may be non-IP traffic through devices such as AWANs and SWANs. TGuardTN keeps these segments secure as well as the IP segments.
- Provides strong encryption including triple DES and AES. Further, encryption algorithms are specifically implemented for NonStop systems to minimize resource requirements and ensure high performance.
- Choices for Key Management - TGuardTN provides a choice for key management, fixed key and dynamic key exchange. Fixed key allows keying material to be stored in the clear. TGuardTN then generates the fixed key from the keying material. Dynamic key exchange uses Diffie-Hellman key exchange to allow session keys to be exchanged securely.
- Application transparency - no changes are required for any application to be able to use TGuardTN.
- Multi-threaded operation - A single TGuardTN process can support multiple sessions (typically up to 256) so your system is not cluttered up with many individual TGuardTN processes.
- Easy installation - Just a few CAIL modules to upload to NonStop. Can be active in a few minutes.
- Choice of clients - TGuardTN works with the CAIL Windows and Plus products as well as the 6530 ActiveX control (that is part CAIL Plus) and within an Internet Explorer environment (with all function keys useable).
- Secure file transfer - TGuardTN automatically secures any file transfers that occur within emulator sessions. This includes IXF and PCFILE transfers.

CAIL Security Facility

B2. TGuardALL - Host Resident Proxy Security - Middleware Encryption (RSC, ODBC, etc.)



Communications Legend: — secure (encrypted) — "clear"

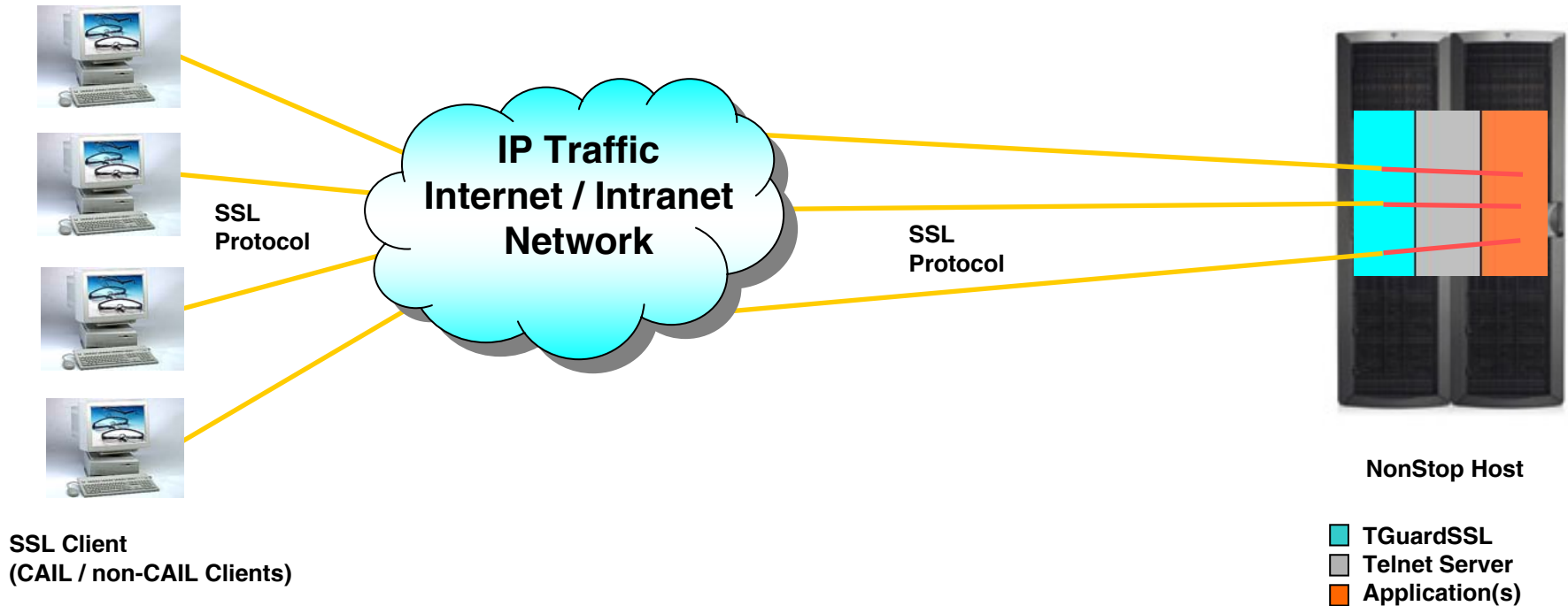
B2. TGuardALL - Host Resident Proxy Security - Middleware Encryption (RSC, ODBC, etc.)

Highlights:

- Front end encryption proxy - TGuardALL provides encrypted data streams transparently for any applications using TCP/IP. Encrypted data is received on a socket and decrypted and passed on in the clear through another socket. The process is reversed for data sent to the remote client. This provides encryption from the remote client to the NonStop system, but not within the NonStop system. Some vendors still refer to this as "end to end" encryption but clear text still appears on a socket connection within the NonStop system.
- Strong encryption including triple DES and AES. Encryption algorithms are specifically implemented for NonStop systems to minimize resource requirements and ensure high performance.
- Telnet and Middleware - TGuardALL can be used to encrypt Telnet or any other middleware protocols such as RSC and ODBC. For Telnet sessions, the CAIL Windows and Plus products (including the ActiveX 6530 control), support TGuardALL automatically. For other middleware protocols, TGuardALL provides PC modules that are installed as a service on Windows based machines. These services need to be started to provide the encryption services on the PC.
- Choices for Key Management - TGuardALL provides a choice for key management, fixed key and dynamic key exchange. Fixed key allows keying material to be stored in the clear. TGuardALL then generates the fixed key from the keying material. Dynamic key exchange uses Diffie-Hellman key exchange to allow session keys to exchange securely.
- Application transparency - no changes are required for any application to be able to use TGuardALL.
- Easy installation - Just a few CAIL modules to upload to NonStop. Can be active in a few minutes.
- Multi-threaded operation - A single TGuardALL process can support multiple sessions (typically up to 256).

CAIL Security Facility

B3. TGuardSSL – SSL Host Resident Proxy Security



Communications Legend: — secure (encrypted) — “clear”

B3. TGuardSSL – SSL Host Resident Proxy Security

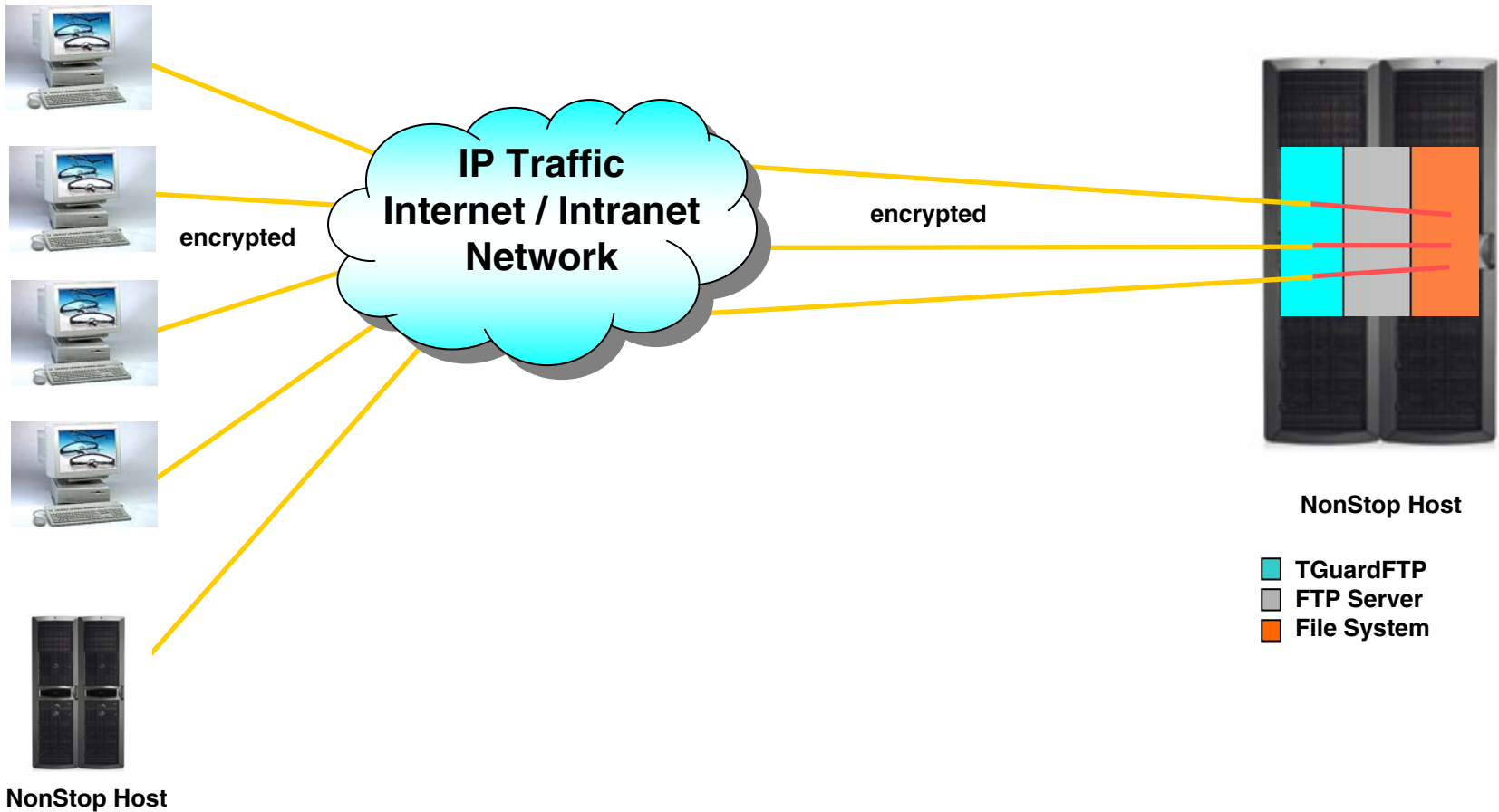
Highlights:

- Front end SSL encryption proxy - TGuardSSL provides a host resident proxy that implements the SSL standard for TCP/IP based applications. This proxy provides authentication, encryption, and authorization services for telnet sessions. Encrypted data is received on a socket and decrypted and passed on in the clear through another socket. The process is reversed for data sent to the remote client. This provides encryption from the remote client to the NonStop system, but not within the NonStop system. Some vendors still refer to this as "end to end" encryption but clear text still appears on a socket connection within the NonStop system.
- Strong encryption including triple DES and AES.
- Application transparency - no changes are required for any application to be able to use TGuardSSL.
- Easy installation - Just a few CAIL modules to upload to NonStop. Can be active in a few minutes. Installation will be slightly more complicated if server authentication is being utilized.
- Multi-threaded operation - A single TGuardSSL process can support multiple sessions (typically up to 256).

Secure Systems

B4. TGuardFTP - FTP Host Resident Proxy Security

Windows, Browser or Java Client (CAIL / non-CAIL Client)



Communications Legend: — secure (encrypted) — "clear"

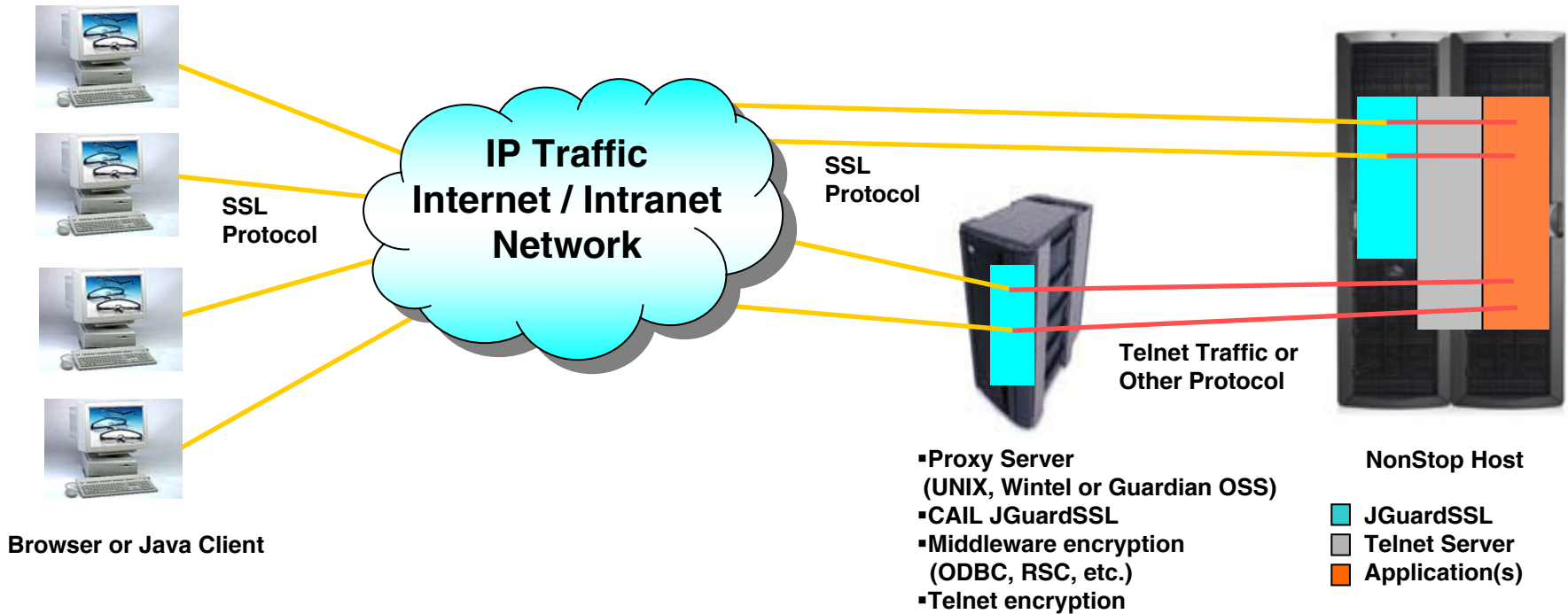
B4. TGuardFTP – FTP Host Resident Proxy Security

Highlights:

- Front end encryption proxy - TGuardFTP provides support for encrypted data sessions that use the FTP protocol. FTP sessions can be from a PC to a NonStop or between NonStop systems. Encrypted data is received on a socket and decrypted and passed on in the clear through another socket. The process is reversed for data sent to the remote client. The FTP protocol requires its own proxy since any FTP encrypted data that traverses a firewall or NAT translation device prevents the firewall or NAT device from determining the ports that will be used by the remote client for data connections (these must be allowed for the FTP transfer to occur).
- Strong encryption including triple DES and AES. Encryption algorithms are specifically implemented for NonStop systems to minimize resource requirements and to ensure high performance.
- Support for TGuardFTP built into CAIL / Windows, CAIL / Plus and the CAIL ActiveX control.
- FTP client transparency - no changes are required for any FTP client to be able to use TGuardFTP.
- Easy installation - Just a few CAIL modules to upload to NonStop. Can be active in a few minutes.

CAIL Security Facility

B5. JGuardSSL - Java SSL Proxy Security



Communications Legend: — secure (encrypted) — "clear"

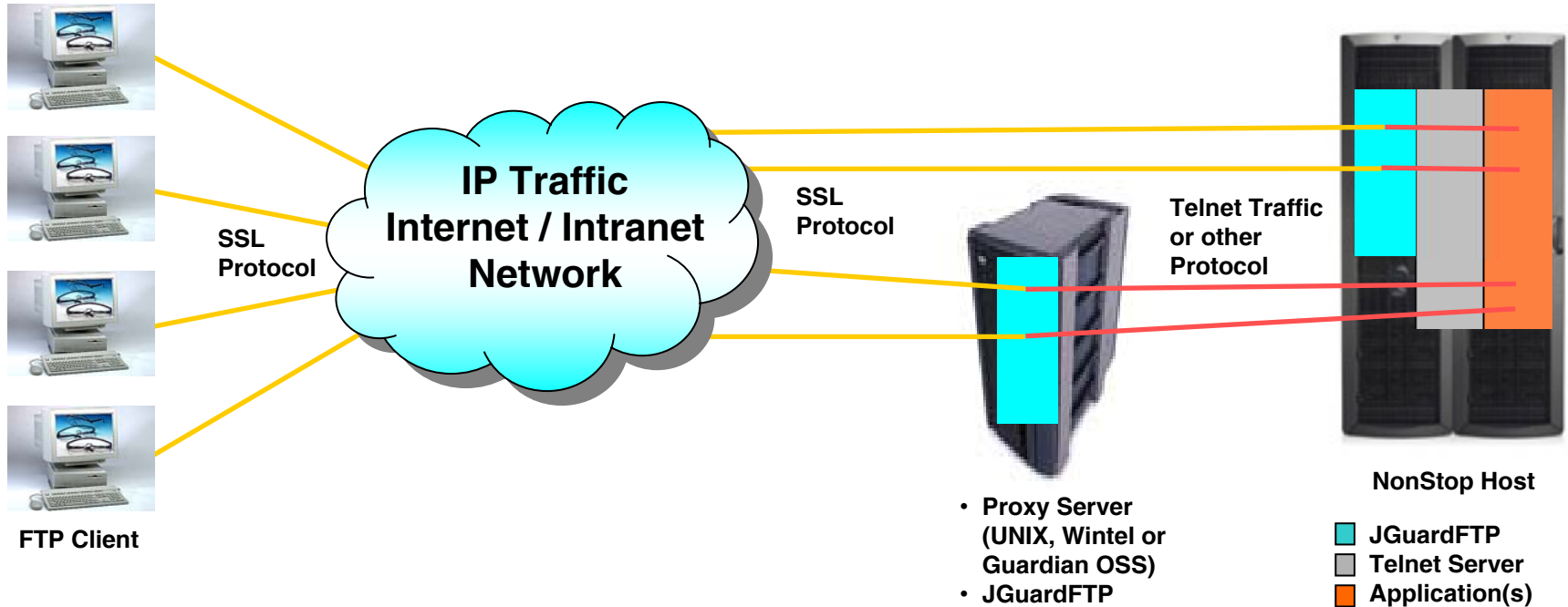
B5. JGuardSSL – Java SSL Proxy Security

Highlights:

- Front end SSL Java encryption proxy - JGuardSSL provides a front end proxy with a Java implementation of the SSL standard for TCP/IP based applications. This Proxy provides authentication, encryption, and authorization services for telnet sessions. Encrypted data is received on a socket and decrypted and then passed on in the clear through another socket. The process is reversed for data sent to the remote client.
- Economical front end - JGuardSSL can be installed on a UNIX or Windows box that sits in front of a NonStop system. This can serve as a very inexpensive alternative to SSL hardware encryption devices. It can also serve to off-load expensive NonStop CPU cycles to less expensive boxes.
- NonStop OSS front end - JGuardSSL can also be installed on any NonStop system that uses OSS.
- Strong encryption including triple DES and AES.
- Application transparency - no changes are required for any application to be able to use JGuardSSL.
- Easy installation - Just a few CAIL modules to upload to NonStop. Can be active in a few minutes. Installation will be slightly more complicated if server authentication is being utilized.
- Multi-threaded operation - A single JGuardSSL process can support multiple sessions.

CAIL Security Facility

B6. JGuardFTP – Java SSL FTP Proxy Security



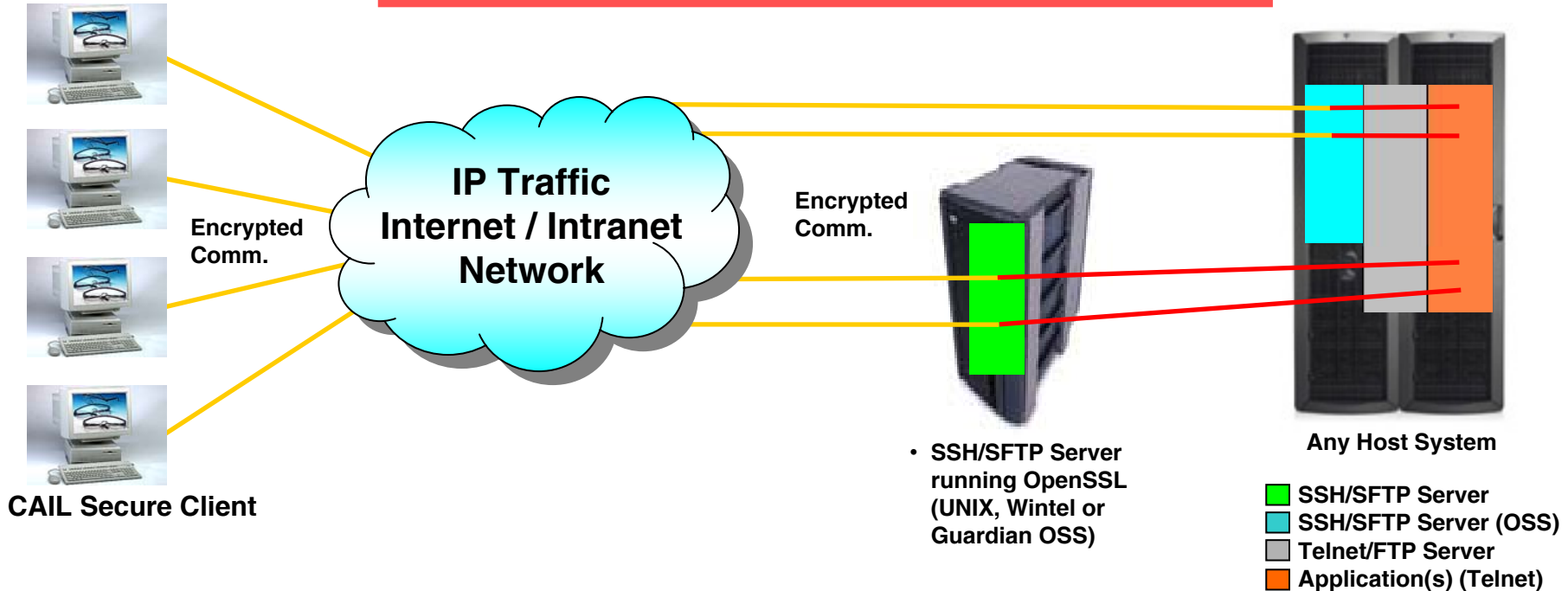
Highlights :

- Can secure any FTP Client
- Very fast SSL standard for FTP
- Any Host to any Host secure file transfers (with Java 1.3 or above)

Communications Legend: — secure (encrypted) — “ clear “

CAIL Security Facility

B7. SSH / SFTP Client for UNIX

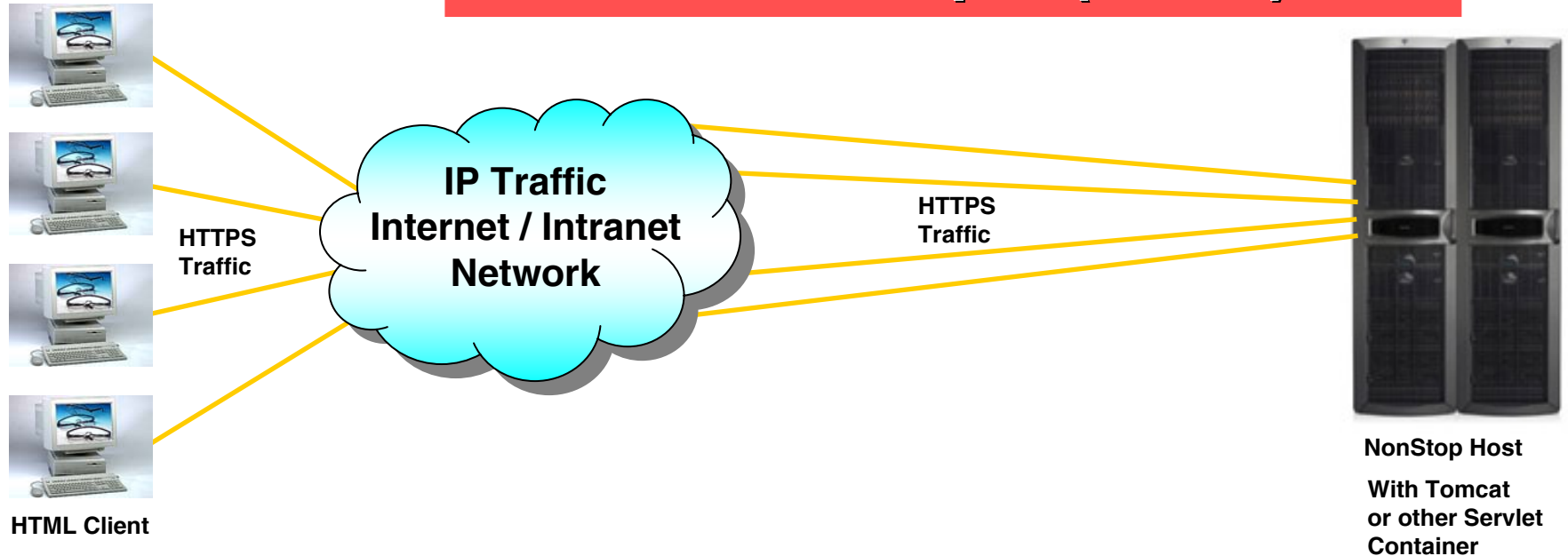


Highlights :

- End to End secure Direct SSH for VT 100 – Transparent no changes to applications
- SSH Tunneling for 6530 sessions
- SFTP standard file access in GUI FTP environment

CAIL Security Facility

B8. CAIL XML Adapter (HTTPS)



Highlights :

- NonStop Server not directly available to the outside world
- Encrypted HTTP traffic from client to WEB server
- Works with any Browser
- GUIized screens – simple to edit XSL Files
- Consolidate screens using modified front ends

Communications Legend: — secure (encrypted) — “ clear “

CAIL

CAIL Security Facility

C. Summary

Features	Benefits
1. Browser based Java, ActiveX, or Windows access	Employ powerful and flexible secure communications, or programmable Java and ActiveX solutions
2. SSL option using CAIL Security Facility	Standardized secure methodologies using modular Java components, optionally use separate machine to house CAIL Proxy reducing Host processing load, and hiding Host address
3. DES and AES encryption	“End-to-End” secure sessions Selectable encryption levels to balance processing load with security mandate
4. Key Management - Fixed Key - Diffie-Hellman Exchange	Security that is efficient and economical Full security communications model with no key management administration
5. Encrypt Middleware	SSL / TLS compatibility standard (includes FTP and tunneling) Utilize CAIL security on NonStop for RSC or other Socket Protocols
6. Easy to Install or Deploy	Can be active in minutes
7. Modular Security Components	Seamless integration with Network, Web and Dial-In Hosts Transparent to users No application changes or additional hardware
8. Scalable	From a few desktops to the enterprise

CAIL Security Facility

C. Summary - Conclusions

CAIL enables you to have more trusted systems:

1. easily, quickly and economically
2. support for
 - Windows and Browser clients
 - File Transfers
3. choice of
 - encryption technologies
 - implementation (deployment strategies)

.... to address Security requirements - today and in the future