

Realtime
publishers

"Leading the Conversation"

The Shortcut Guide[™] To



Securing Automated File Transfers

sponsored by



Ed Tittel

Chapter 4: Compare/Contrast SFTP, FTPS, and IPsec.....	68
Host-to-Host VPNs	69
Host-to-Gateway VPNs	69
Gateway-to-Host VPNs	69
Gateway-to-Gateway VPNs.....	69
Software Solutions	70
Hardware Solutions.....	70
Intranet Solutions	71
Extranet Solutions.....	71
Tunneling Protocol Options.....	72
Advantages.....	72
Disadvantages	74
Security Considerations	76
Strong Encryption and Authentication Using Standard Algorithms.....	76
Consider How Control and Data Channels May Be Handled.....	77
Security Policy and Compliance Requirements.....	77
When to Use SFTP.....	78
When to Use IPsec	78
When to Use FTPS.....	79
Security	79
Flexibility	79
Certificates and Certificate Authorities	79
The Demilitarized Zone	80
FTP Placement Inside the Firewall.....	80
Choosing a File Transfer Solution	81
Total Cost of Ownership.....	81
Assessing Overall Applicability	82
Summary	83

Copyright Statement

© 2007 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

Chapter 4: Compare/Contrast SFTP, FTPS, and IPsec

In previous chapters of this book, we've examined the issues involved in finding and replacing or strengthening the types of file transfers used for so many important tasks in so many enterprise settings. Along the way, we've dug into various key tools and technologies that may be used to help this effort along. Key elements in this laundry list of possibilities have included the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) as well as IP Security (IPSec) and the ever-popular Secure Shell (SSH, which today includes both SSH-1 and SSH-2 versions). We've also explained how these various elements may be employed to help boost security for file transfers and to assure reasonable levels of security, confidentiality, and control over file transfer activities and the content and control information they typically convey.

In some cases, it may make sense to simply wrap existing implementations—such as scripts; legacy tools; or other file transfer code for which there may be no source code available nor an easy way to remove older, less secure file transfer applications such as FTP—and to replace them with more secure alternatives such as SFTP or SCP. These are cases in which adding an extra security wrapper, such as IPSec or SSL/TLS can provide the kinds of security, confidentiality, and control that the file transfer programs (and other code inside the wrapper) may lack.

In fact, a Virtual Private Network (VPN) comes very close to realizing the old puzzler about how to have one's cake and eat it too. That's because proper use of VPN technology permits public networks—most notably, the Internet—to serve admirably and securely for ferrying private, encrypted communications between senders and receivers. In fact, the more the VPN software can direct traffic through its transports, the more secure ordinary network communications become, especially those that may not be very secure (or secure at all, such as FTP, Telnet, and unencrypted email clients).



The connection medium used to distribute information is a major determining factor when choosing a VPN solution. Part of this choice is platform-specific and another part is protocol-specific.

The type of VPN arrangement required between each participating endpoint is another major factor to consider when deciding on a solution. There are connection endpoints, or those that establish actual VPN connections from one network to another, and data endpoints that send and receive private information across VPN links. In some situations, these two entities may be part of the same unit or spread across several separate units.

Host-to-Host VPNs

Host-to-host VPN is designed to replace costlier frame-relay and leased-line arrangements that might otherwise be used to secure communications between the host's business partners, subsidiaries, subscribers, or vendors. This configuration provides end-to-end security as the VPN software is installed on each host computer that runs whatever applications that need more security, including file transfer.

Host-to-Gateway VPNs

In a host-to-gateway arrangement, the VPN protects data in transit between a host on some local network segment and a remote gateway device—but not data on the remote network. This may also be called a remote access VPN. However, please note that this configuration only secures part of the communications link and does not provide complete, end-to-end security (though ideally it secures all public links across the Internet, which are presumably in greatest need of security and enhanced protection).

Gateway-to-Host VPNs

In a gateway-to-host VPN, one endpoint consists of a network serviced by an intermediary VPN gateway endpoint that communicates with a single remote network contact over an intervening network. Data moves between gateway and host endpoints under the protection of VPN-supplied encryption but traverses the local network segment behind the gateway unmodified. Likewise, this configuration only secures part of the communications link and does not provide complete, end-to-end security.

Gateway-to-Gateway VPNs

Gateway-to-gateway implies that both connection and data endpoints differ in their VPN topologies. Traffic is protected between connection endpoints but travels in native form in either direction between data endpoints. This may also be referred to as a site-to-site VPN, or mutual interconnection between entire networks.

As a usage scenario, consider an organization comprised of a single central office with several branch offices, all of which maintain their own intranets. VPN protection is mandated for safe passage of information across the Internet but not within each respective intranet. A series of border servers acting as VPN gateways can exchange information securely and freely with every other recognized and valid intranet through the intervening network medium (the Internet).

Software Solutions

Software-based VPNs require a computer capable of handling intensive encryption and compression routines above and beyond whatever existing desktop or server applications may already be in use, with minimal impacts on system performance and application responsiveness.

Security becomes more challenging as the number of VPN installations increases. Likewise, as the VPN orientation focuses on either internal or external communications if not both ways, complexity likewise increases. When establishing matched system architectures, similarity among load-balanced systems must be carried to the logical extreme. Each platform must use identical hardware, and software images must be compatible down to the patch-level (for cloned or clustered servers) and for all access permissions. As the old saying goes, one rotten apple can spoil the whole barrel: the same thing is true for each and every system in a load-balanced group—namely, that mismatched elements can cause instability problems, severely degrade performance, or cause load balancing to fail altogether.

Each installation must be considered at risk in varying degrees according to its orientation toward internal and external sources. The security of any VPN solution is directly impacted by the supporting operating system (OS) environment, which must therefore be taken into consideration for each and every installation. This issue affects both client and server roles in any VPN arrangement equally.

Hardware Solutions

Certain intermediate network appliances are specifically designed to offload VPN processing from host machines. Such appliances may be placed inline on the network, and provide a viable and workable VPN solution particularly for medium- to large-scale network environments. VPN appliances dutifully handle encryption, compression, and other VPN-related tasks, thus accelerating the performance of VPN-based network transactions. One caveat that applies to vendor-specific VPN solutions, whether hardware or software oriented, is that one vendor's IPsec implementation may not always work with another's. There are VPN routers and appliances on the market that may be compatible only with identical makes and models. Thus, you must match these devices on either side of the network connection that they straddle. You'll want to investigate detailed product specifications and disclaimers carefully, and make your selections accordingly. Where homogeneous components may be neither feasible nor desirable, you will need to test candidate configurations carefully to make sure things work properly before deploying any equipment into the field. Essentially, this means setting up a test lab that resembles the planned deployment environment as much as is technically possible, and subjecting it to usage scenarios and workloads that also match the target networks. Only those solutions that actually work, and work sufficiently well to meet user requirements, should ever reach users' hands.



It is worth noting that most hardware solutions, if any, also do not provide complete, end-to-end encryption.

Intranet Solutions

Business assets may be (and usually are) dispersed over multiple, disjointed regional territories. Nevertheless, each location can use dedicated equipment to establish VPN partnerships between pairs of sites (or between spoke ends and hubs, in the hub-and-spoke model). Branch and central offices can be mutually conjoined across the Internet by using a VPN solution.

This approach offers significant cost savings as compared with pricier frame-relay or leased-line arrangements (as explained earlier, the savings can be substantial, even when additional services are included in the mix, often on the order of thousands to tens of thousands of dollars per month for medium- and enterprise-class organizations). However, please bear in mind that gateway solutions may not provide you with the level of security you need. Remember that to be 100% protected, you must ensure that your VPN solution provides complete, end-to-end (application-to-application) security.

Extranet Solutions

Business alliances may encompass two or more companies closely cooperating with intranet-based VPNs to coordinate and provide specialized services to customers and clients. This affords such companies the ability to interoperate within a mutually shared and secured environment via the Internet to enhance business operations and provide applications and services that take advantage of their combined information and processing assets.

An extranet solution is probably best characterized as providing additional Layer-3 security to extend wide area networks (WANs) to other regional territories or business partnerships. Because the sum of the security risks across multiple organizations is greater than the individual risks that each participant must shoulder, owing to additional exposures and vulnerabilities that appear “in the cracks” between organizational boundaries and controls, this helps to explain heightened needs for authentication, access controls, security, and auditing that are typical for extranets—and in the VPN environments that support them.

 For more information about Layer-3 security in VPNs, see the Cisco white paper “[Beyond the Basics: Technologies for Compelling Layer 3 VPN Services](#).” Tim Greene’s Network World story “[Layer 2 vs. Layer 3 VPNs](#)” zeroes in on issues specific to MPLS in this regard, and may also be of interest.

Tunneling Protocol Options

As described in the preceding chapters, many types of protocols may be used to create secure tunnels between pairs of endpoints. That said, we only explore IPsec, SSL/TLS, and SSH here, as we discuss their respective advantages and disadvantages as they relate to securing automated file transfers

Tunneling requires a carrier protocol, an encapsulating protocol, and a passenger protocol. The carrier protocol is used by the network upon which information travels, and the encapsulating protocol envelops the passenger protocol, which includes all data being transported.

It is important to understand the primary distinction between an IP-layer tunneling mechanism such as IPsec and a higher-level counterpart such as SSL/TLS or SSH: high-level services protect a single protocol and low-level services protect a single link.

In the case of SSL/TLS and SSH, these higher-level services safeguard individual protocols such as FTP, Telnet, SMTP, and so forth, most typically on a one-at-a-time basis. For a lower-level framework, such as IPsec, anything may traverse the link it envelops—even protocols that may not be routable can be encapsulated easily and transparently for delivery across the tunnel.

Advantages

There are numerous protocols used for tunneling which may be used to create VPNs. As this guide largely concerns the distinctions between IPsec, SSH, and SSL/TLS solutions, only those options are explored.

Advantages of IPsec

IPsec has its relative strengths and merits, particularly in the enterprise computing environment. Chief among these are the following:

- Protects any protocol—IPsec uses IP for multi-protocol encapsulation
- Protects any medium—IPsec utilizes multi-protocol encapsulation over any single-protocol medium
- Total transparency—IPsec background services have no visible impact on end users
- Total scalability—IPsec can be applied to different networks of various sizes and capacities
- Total independence—IPsec will route any number of network-based applications
- Connection-class controls—IPsec supports network-based authentication
- Economy of bandwidth—IPsec supports compression for improved throughput
- Protocol bridging—IPsec provides multi-protocol local networks across a single-protocol backbone
- Connectivity solutions—IPsec provides workarounds for networks restricted by limited hop counts such as Appletalk or NetBIOS
- Total network continuity—IPsec interconnects discontinuous subnetworks
- Extended coverage—IPsec allows VPNs to operate across WANs

Advantages of SSL

SSL also has numerous interesting noteworthy aspects, as the following list highlights:

- Completely universal—SSL's all-purpose applicability instantly creates a VPN client using any modern Web browser (older versions may not support SSL, so be sure to test older browsers that may be employed in your user population, knowing that VPN requirements may force upgrades to occur)
- Total flexibility—SSL supports additional applications without firewall configuration changes
- Total transparency—SSL background services have no visible impact on end users
- Cost effectiveness—Existing SSL implementations conserve both time and budget
- Unrestricted movement—Many SSL VPNs use the SHTTP port, allowed to pass through most firewalls

Advantages of SSH

As a protocol originally developed to replace remote logins, terminal emulation, and remote login, SSH excels at enabling users to get things done via secure remote access. Enhancements added since its inception in 1995 enable this protocol to support tunneling and port and X11 connection forwarding, and sets up a secure, encrypted channel between local and remote hosts, with strong authentication from user to remote host and vice-versa. SSH protects message content and ensures message integrity via encryption for confidentiality and message authentication codes for integrity. Other advantages include the following:

- Easy to deploy and maintain
- Virtually all computing platforms are supported from Windows to mainframes, where nearly all of these versions interoperate very well
- Provides true end-to-end security for the applications it protects
- Provides supports for strong two-factor (or multi-factor) user authentication
- Provides authentication for computing hardware (for example, servers and hosts) as well as users
- Commercial implementations offer advanced features including tools to automate replacement of scripted file transfers with secure alternatives
- Port forwarding may be used to transparently secure file transfers, when replacing insecure FTP with secure alternatives (SFTP, SCP) isn't an option
- Easy to secure HTTP-based or homegrown file transfer applications without altering programs already in use
- Works with IPsec and SSL VPNs without requiring substantial alterations on either side of that interaction
- Can be used to protect virtually any application, so once you have decided on SSH, you have a protocol that can solve many security issues at the same time; it not only enables easy replacement of FTP but also helps to solve the Telnet problem

Disadvantages

There are also disadvantages to using either IPsec, SSH, or SSL/TLS for securing a network environment. As is the case with virtually any security solution, measurable benefits relate to how well and completely any product addresses security concerns and conditions.

Disadvantages of IPsec

Among other implementation-specific challenges, IPsec is subject to the following distinct disadvantages:

- Various implementations are not necessarily compatible, especially when using out-of-the-box defaults, and can require significant testing and deployment time
- IPsec is only as secure as the gateways through which it passes—vulnerable intermediate devices can undermine trust
- Not secure end-to-end—IPsec secures two endpoints, not applications and users
- Endpoint-oriented—For IPsec, strong authentication functionality operates without user IDs
- Not fully featured—IPsec lacks digital signatures and public key functionality
- Not unobservable—IPsec is not designed to defend against traffic and protocol analysis
- Intrusive—For IPsec, OS integration at the network level is required for it to be usable
- Expansive—For IPsec, encryption of small packets produces large overhead to payload ratios

Likewise, SSL presents its own unique challenges and considerations when it comes to solving the security equation:

Disadvantages of SSL

SSL requires much more effort on the part of the end users to establish an ad hoc trust relationship for the purpose of exchanging messages, information, or data. Although this is more convenient from an administrative standpoint, it's also an inconvenience in that typical network-level authentication mechanisms do not directly apply to such traffic (as is the case for IPsec).

The following list highlights additional disadvantages of SSL:

- Inherently insecure—Each SSL implementation is only as secure as the local computer on which it runs
- Inherently incomplete—For SSL, strong authentication is required for enterprise-grade VPNs
- Untrusted sources—For SSL, administrators cannot specify privileges using client origin IP addresses
- SSL VPN solutions secure Web-based applications by default, but additional software must be installed on each PC to provide more advanced functionality
- Rarely provides end-to-end protection as SSL VPNs normally use a client-gateway architecture

Disadvantages of SSH

SSH was not originally designed as a VPN, though it works to deliver much of the same functionality that VPNs offer, most importantly, a secure connection. SSH is a software product and as such needs to be installed and configured. Other disadvantages of SSH include:

- The most secure and advanced implementations of SSH are commercial, especially where automation tools and infrastructure extensions may be needed or desirable (for example, for automating switchover from insecure file transfer applications to more secure alternatives)

 SFTP and SCP are part of SSH and are included as an integral part of commercial products.

- SSH is not integrated at the OS level, so software will have to be installed on most platforms

In actuality, SSL/TLS and IPsec solutions can coexist quite happily in secure network environments and represent cogs in a much larger-scale security infrastructure. SSH often serves as an alternative or replacement for either or both schemes, because it is simpler, less costly, and less labor-intensive to implement. That said, SSH also coexists quite successfully with IPsec and SSL/TLS technologies.

Protocol	Pros	Cons
IPSec	Protects individual links	Costly, difficult to implement
	Encapsulates all kinds of protocols	Differing vendor defaults cause problems
	Protects any protocol	Gateways provide points of exposure
	Protects any medium	Secures endpoints, not applications or users
	Transparent to end users	Authentication works without user IDs
	Highly scalable	Lacks digital signatures, full PKI support
	Application independent	Does not defeat traffic/protocol analysis
	Works with network-based authentication	OS must be integrated at network level
	Supports compression	IPSec VPNs are normally deployed in gateway-gateway configurations and do not provide full end-to-end security
	Interconnects discontinuous subnets	All implementations are not NAT friendly
	Enables VPNs to operate across WANs	Heavy overhead encrypting small packets
SSL/TLS	Works with modern Web browsers	Only as secure as computers it runs on
		Does not necessarily provide end-to-end support for legacy applications such as FTP
		Does not provide support for non-Web applications without installation of additional software.
		Often reliant on OpenSSL libraries
	Add applications without firewall changes	Lacks built-in strong authentication
	Background services don't impact users	No privileges associated with client IP
	SSL implementations save time and money	More effort to establish trust relationship
	Use SHHTTP port to bypass firewalls	Network-level authentication does not apply

SSH	Supports various types of remote login	Not originally designed for VPN use
	Support various forms for authentication, including password, public/private keys, certificates, RSA Secure ID, Kerberos, GSSAPI, PKI, and so on	Must be integrated with authentication
	Supports tunneling	
	Forwards X11 connections & TCP ports	Most secured implementations are proprietary
	Uses SFTP or SCP for secure transfer	Some expense, upkeep involved
	Confidentiality and integrity built-in	Apps may be needed to secure transfer/copy
	Easy to deploy and maintain	Not integrated at OS level
	Easy automating secure transfers, scripts	
	Port forwarding transparently secures xfer	
	Easy to transparently secure HTTP apps	
	Works with IPsec VPNs	
	Works with SSL/TLS VPNs	
	Delivers true end-to-end security	

Table 4.1: Summary of tunneling protocol pros and cons.

Security Considerations

There are many elements to consider when establishing or enforcing an overall security scheme. Policies, procedures, and people's roles all must be defined so as to operate in some particular capacity, with some set of restrictions, and under some formal method to ensure proper compliance and regulatory controls are in place. Each element must be broken down into its basic parts and defined according to the roles it fills. Every component must be scrutinized and defined according to its terminology, rules, and processes.

Strong Encryption and Authentication Using Standard Algorithms

The use of strong encryption provides additional security against skilled and brute-force attempts to gain access to securely encrypted data. The use of standard algorithms ensures a reasonable level of resilience to such attacks when applying appropriate keys or passwords of appropriate bit strength. Implementing strong access controls provides the authentication necessary to safeguard against and account for potentially hostile user activities.

 Standard encryption algorithms are published and knowledge about their operation is widespread. Most security experts believe that such openness leads to widespread efforts in the security community to expose and deal with weaknesses, vulnerabilities, and exposures, and rapid abandonment of algorithms deemed not worth saving, repairing, or maintaining. Proprietary or closed encryption algorithms often turn out to be weaker, and the results of their compromise more severe, because the lack of openness does not foster common understanding of and appreciation for their strengths and weaknesses. Examples of standard security algorithms include DES, triple DES, RC4 and RC5, and the Advanced Encryption Standard (AES).

Both encryption and authentication play a critical role in a much larger security picture: together, they establish a firm foundation for trust between servers, services, and subjects. As such, they should use only established, standard algorithms to ensure reliable and safe operation. As a rule, standard algorithms must withstand lengthy and thorough public reviews, private audits, and widespread inclusion with other security applications and services, which has the added benefit of ensuring interoperability among multiple platforms and architectures.

Buying into a non-standardized implementation potentially ties an organization into a vendor-specific viewpoint that may not scale well or adapt to changing conditions such as business mergers, acquisitions, or newly formed partnerships. Where possible, buyers should seek out certified solutions for deployment (in the US, this would mean preferential selection of implementations certified to comply with FIPS 140-2, for example).

 For various lists of products validated to conform to FIP 140-2, please visit <http://csrs.nist.gov/cryptval/vallists.htm> (especially the FIPS 140-1 and FIPS 140-2 Vendor List).

 In his classic security book *Secrets & Lies: Digital Security in a Networked World*, security maven Bruce Schneier makes the point that “if a [security] primitive is only secure if it remains secret, then it will only be secure until someone reverse engineers and publishes it.” He goes on to point out that proprietary security primitives that have been so outed include digital cellular communications encryption, DVD encryption, FireWire encryption, various Microsoft encryption algorithms, various smart card electronic commerce protocols, the secret hash function in SecureID cards, and even the protocol that protects Motorola’s mobile MDC-4800 Police Data Terminal. His most telling point is that “public primitives are designed to be secure even though they are public; that’s how they’re made. So there’s no risk in making them public.”

Consider How Control and Data Channels May Be Handled

Keep in mind that a solution such as FTP via SSL/TLS is a patchwork fix to a much more complex problem than it can address. Remember that with FTPS, the control connection is always encrypted but the data channel may not be likewise secured (in other words, account and password information will be protected but the contents of files transferred may be sent in the clear, which provides some improvement over plain-vanilla FTP, but still exposes files to snoopers). Because the authentication process must be fully protected at all times, it should support full-time use of encryption to thwart eavesdropping attacks against the system by intermediary devices or parties. That said, pre- and post-process encryption files do affect how they will be handled in transit. In the first case, a pre-processed encrypted file passes through the data channel unmodified; in the latter case, a file must be processed prior to its transmission across the network medium and incurs a performance penalty.

Security Policy and Compliance Requirements

The goal of any security or privacy policy is simple: to help employees *do the right thing*. All security and privacy policies must take into account regulatory requirements during the drafting, designing, or updating process. Not only must such access and administrative controls already exist for many organizations, they must also be demonstrably compliant with HIPAA, SOX, or whatever legislation, regulations, or contractual agreements with third parties that may apply to the organizations in question.

When to Use SFTP

SFTP is built upon SSH and provides an additional secure encapsulation of file transfer command and data streams. SFTP uses the existing SSH protocol to create and manage multiple command and data streams to safeguard against eavesdropping by intermediate parties that may attempt to harvest sensitive information, including login credentials and files.

SFTP may be used anywhere SSH is implemented in client or server form. Both console and graphical clients are available for most OSs, which makes SFTP an excellent fit for most enterprises and inter-organizational arrangements. Use SFTP readily wherever plain-vanilla FTP installations need a security upgrade. This means you should deploy SFTP where personal identity information or business-critical confidential data may be acquired, retained, or processed, as when handling medical or financial records or when transferring proprietary or sensitive data among business partners (or between sites inside some organizations). In fact, it's a prudent practice to consider SFTP first before turning to stopgap measures such as FTP over SSL/TLS solutions because SFTP offers better security and is often easier to manage than such other alternatives.

It is interesting to note that many organizations now use SFTP exclusively across their enterprises to secure all data in transit once and for all. Overall security risks may be reduced significantly when using software such as SSH Tectia on each computer in the network, and it is a cost-effective way to secure just about any network. One conclusion that may be drawn from these observations is that SFTP should be used whenever an organization seeks to secure its data with no (or in the worst case, only minimal) changes to its applications or infrastructure.

When to Use IPsec

IPsec is best deployed in situations in which complete access to hardware and local software, including modification of the OS and related administrative utilities, is permitted. Network-based authentication makes IPsec most suitable for connection-oriented access and authorization controls but a poor choice for client-oriented permission granularity. Thus, IPsec might be best suited for securing conferencing or chat-type interactive applications, but some other approach that integrates access control lists (ACLs) or role-based security might work better for providing remote access to file stores or document repositories.

That said, IPsec should invariably be used in concert with other site-specific security measures. Firewall configurations, intrusion detection systems (IDSs), and possibly user-held identity tokens or biometric identification devices may also be necessary to establish the right levels of enterprise security. Likewise, the processing demands that large user communities can impose on network access and transfers may also mandate deployment of intermediate network appliances as well to handle encryption and decryption, help with authentication and identity management, serve as remote access gatekeepers, provide VPN support, and so forth.

When to Use FTPS

FTPS involves the use of a separately created secure channel with an existing, full-fledged FTP server by adding another, secure file transport layer based on SSL/TLS. Essentially, this method adds SSL-capable send-and-receive functionality to existing FTP protocols and server applications. However, this approach only partially addresses FTP security issues, which lacks other strong components that are routinely included as part of an SSH/SFTP subsystem. Strong authentication and user-based transaction accounting are two primary examples of what else comes as part and parcel of such offerings, and helps explain why these kinds of solutions have proved so popular in enterprises and organizations of all sizes and scales.

Security

Standard SSH provides a remote login shell for the user. It is possible to restrict how this shell behaves for those clients—that is, to more precisely specify what types of access and actions will be permitted and which ones may be denied. Setting up a more customized shell environment for clients may require more complex SSH server configurations. FTPS, however, offers no ability to execute arbitrary commands outside those built-in to the FTP command set. Here again, the neatly compartmentalized implementation that FTPS delivers helps to explain its widespread popularity and use.

 For information about how to restrict SSH access, see <http://www.snailbook.com/faq/restricted-scp.auto.html>.

Flexibility

Because FTPS is a straightforward extension of the existing FTP infrastructure, it is supported in many proprietary and open source server applications. In fact, enabling FTPS in most of these services usually involves setting only a simple configuration parameter. No additional firewall configuration or supportive services are needed.

Certificates and Certificate Authorities

Where SFTP uses keys or certificates (among other mechanisms), FTPS uses certificates. FTPS does not support the chains of trust paradigm facilitated through Certificate Authorities (CAs), nor does it require that parties first exchange confidential security details before forming a trust relationship. That said, SSH supports a wide range of authentication mechanisms, including client keys (which must be maintained on the server) and certificates issued by CAs both public and private.

The Demilitarized Zone

In relation to computer security, a Demilitarized Zone (DMZ) refers to a network segment that resides between an internal and external network, such as when an FTP, Web, or database server is located just outside the intranet but between the internal intranet and the external Internet. Typically, a DMZ contains devices that are Internet accessible on a specifically designated subnet that is isolated from protected internal resources. There may be one or more DMZs, separated by firewalls, each housing separate servers running different services; for example, one DMZ for HTTP servers and another for public DNS and SMTP.

FTP Placement Inside the Firewall

The firewall plays an integral role in monitoring and controlling network traffic that passes in and out of any organization's perimeter. A typical one-tiered configuration places LAN endpoints (clients and servers) in close proximity to the network, separated perhaps only by a firewall or perhaps a router. Administrators can log in and supervise FTP behavior easily by placing the server inside the firewall. Traffic flow between DMZ segments, LAN endpoints, and Internet-reachable destinations can be captured, observed, and adjusted quickly as needed.

A two-tiered architecture includes front-end client-oriented servers and back-end server-oriented servers, perhaps contained within a single DMZ or perhaps separated by an internal firewall or router with active ACLs. This arrangement is suitable for most business networking environments although banking, financial, and health institutions may require more robust security configurations, as described further in the following paragraph.

Three-tiered architecture begins with a front-line assembly of client-oriented service application servers and middle-man application servers that negotiate transactions between front-end servers and better protected back-end servers. These layers may be called the presentation, business, and back-end tiers, respectively. Business and presentation tiers reside in a DMZ behind an Internet-facing firewall, with discrete firewalls separating them from the back-end tier. This arrangement provides more granular control over network-based application transactions than with one- or two-tiered configurations, where information can be checked, controlled, and handled separately at each point in the transaction chain.

Choosing a File Transfer Solution

Ultimately, the file transfer solution you choose will be determined by your specific business needs and the kinds of connectivity that extranet and remote access requirements entail. Local compliance policies and security protocols will help to determine what will and won't work for particular network situations. Whatever those circumstances might be, however, the type and relative sensitivity of data being transferred must also play a key role in driving your selection process.

At-risk servers that house personal identity information (aka personally identifiable information) exert strong attraction on would-be data thieves and require special attention and extra protection. Likewise, sensitive or confidential business information demands additional encapsulation and protection. Prudence and regulation dictate that both types of data assets be afforded strong levels of authentication, access controls, and encryption when such data is stored and whenever it's transmitted to any authorized users. Thus, any file storage and transfer system that may be designated as at-risk or for which a high-threat level is assessed must use a secure file transfer product such as SFTP.

Total Cost of Ownership

Careful risk analysis demands that the cost of your security solution should not exceed the value of the protection it provides and the exposures it helps to avoid or mitigate. The effort involved in performing such risk analysis can exceed the amount of effort involved in the implementation of any security solution that results from such analysis, but the costs of such effort must be considered as you work toward an appropriate solution. The investment decision for endpoint security thus offsets the value of protection and risk avoidance against cost and must budget for the total costs of ownership (TCO) over the useful lifetime of whatever solutions may be included in your organization's security infrastructure.

Both in general and where file transfer solutions are concerned TCO encompasses many elements:

- Security software licensing
- Hardware costs
- Initial deployment labor
- Ongoing maintenance and administration costs
- End-user support and education costs

Despite the widespread use of antivirus and intrusion detection or intrusion prevention software at the enterprise level, viral outbreaks and security breaches do sometimes occur even in enterprise environments. As long as security measures are in place, there is a concomitant need to block any potential countermeasures. On the one hand, information theft occurs much less regularly than do malware-driven incidents (according to statistics from security information clearinghouse IT-Harvest). For example, malware incidents outnumber data theft incidents by at least four orders of magnitude. When you stop to consider the former includes all incidents related to viruses, spyware, and adware and the latter refers only to successful attempts to illegally access unauthorized information, the claim doesn't sound as outrageous as you might think. On the other hand, one single incident of data theft has the potential to cause thousands to millions of dollars of negative financial impact. By enforcing strict policy and regulatory compliance for connecting devices and taking other risk-avoidance, transfer, or mitigation steps as may prove necessary (such as establishing the level of loss an organization is willing to absorb, then obtaining extraordinary loss insurance), proper endpoint security products should provide reasonable protection against tools and automation software that enable attackers to exploit more vulnerable targets.

Cryptographic security is available in various packages whose pricing ranges from free, standardized modular components, to complete, commercially available turnkey solutions that suit a variety of business arrangements and needs. Also remember that when the time comes to decommission or transfer ownership of equipment to third parties, it is essential to cleanse site-specific information, including encryption keys or certificates, from each endpoint computer. Making these vital bits of information accessible to outsiders is like handing the keys to your kingdom to a total stranger.

Assessing Overall Applicability

A well-documented security policy lays the foundation for any secure infrastructure. Such a document, or collection of documents, conveys both intentions and decisions as to the roles that security plays within the organization. A security policy should identify critical and important business resources, activities, and operations. Smaller organizations may have a single security policy document that defines all necessary subjects and objects, where larger organizations may require an overarching general policy document with additional support from additional, specific policy addenda, such as policy documents that govern remote access, firewall behavior, acceptable use, and records and information privacy/confidentiality requirements. Resource usage constraints, remote administration and access controls, and information protection between internal and external sources must all be spelled out in such documentation. All of these topics must be tailored for individual sites, business units, and organizational functions to conform to existing organizational policies and current business needs.



The SANS Security Policy Project (<http://www.sans.org/resources/policies/>) includes a comprehensive set of tutorials, information, resources, and examples of a complete enterprise-level security policy document collection along with information about how to craft and maintain that collection as passing time and changing circumstances will demand.

 The National Institute of Standards and Technology (NIST) offers a collection of [Special Publications](#) that include numerous documents about security policy and related documents and procedures. You can also access two compendia of books on the topic of crafting security policy on SearchSecurity.com—namely “[Security Policy by Example](#)” and “[More Security Policy by Example.](#)”

Summary

Ultimately, securing automated (and other) file transfers within an organization requires finding and identifying the means whereby they occur, and either adding an additional security wrapper to boost security levels or replacing insecure file transfer tools with secure alternatives. Thus, when it comes to designing and implementing secure solutions for file transfer, responsible individuals in enterprises and organizations would do very well to heed the following recommendations:

- Encrypt all data between any two computers involved in file transfer (thereby also implementing end-to-end security, as will be automatically ensured by using SFTP).
- Always encrypt usernames and passwords and publish and enforce proper guidelines for password strength and complexity, providing user education to match.
- Seriously consider how many changes you can make to your file transfer infrastructure. If circumstances dictate little or no changes are possible, SSH is probably the best choice; only if more funds and time are available, should you contemplate implementing other technologies.
- Seriously consider how much time you can allocate to implementing changes to a file transfer infrastructure. IPSec deployments often involve major time and resource commitments, whereas SFTP projects may be undertaken quickly, and normally require only minimal resources.
- Decide how you may best authenticate file transfer processes. If you can leverage existing directory services, such as Microsoft Active Directory (AD), that may make sense. Otherwise, it may be necessary to acquire and implement a public key infrastructure along the lines of PKI.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.