ShareFile Enterprise: Security Whitepaper

CITRIX®

citrix.com

Table of contents

Click on the section names above to navigate to that portion of the book and the arrow icon to return to the table of contents from any page.

Introduction

Citrix ShareFile is an enterprise follow-me data solution that enables IT to deliver a robust data sharing and sync service that meets the mobility and collaboration needs of users and the data security requirements of the enterprise.

Securing data is critical to every enterprise and is a responsibility taken seriously by ShareFile. Savvy IT executives understand that with the plethora of free or low-cost data sharing applications available to end users, it has become critical to provide users with a more secure alternative that still empowers them to sync files across their devices and securely share files with co-workers.

This paper explores the details of how ShareFile is secure by design, and highlights the set of security controls available to ShareFile Enterprise customers.

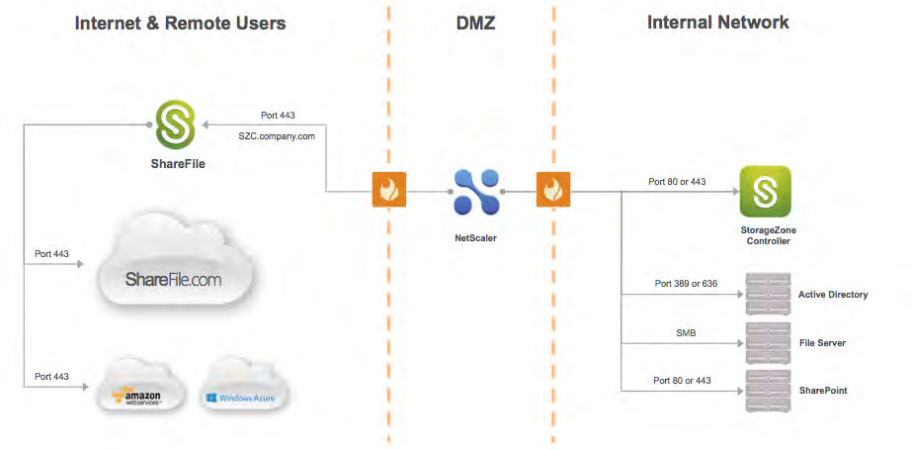

Figure 1: ShareFile components overview with applicable ports.

ShareFile consists of 3 primary components: the SaaS Application Tier, StorageZones, and the client.

1. SaaS application tier – sometimes referred to the as the Control Plane, this is a Citrix-managed component that consists of web, database, and API servers.
2. StorageZones – this is where customer data is stored. Customers have four options when deciding where to store their data. This paper will discuss the workflow and security processes of each option.
   a. Citrix-managed cloud storage on Amazon Web Services.
   b. Citrix-managed cloud storage on Microsoft Azure.
   c. Customer-managed cloud storage on Microsoft Azure.
   d. Customer-managed storage in corporate datacenters.
3. Clients – ShareFile supports a broad device list, which includes but is not limited to Windows and Mac OSX, Android and iOS, Windows phone and Windows Metro.

SaaS application tier

ShareFile servers: Web, API, and database overview

The ShareFile SaaS application tier is hosted in Citrix's datacenter. The components include (see figure 2.):

- NetScaler – used to load balance client requests to the ShareFile.com/eu webs and API web servers.
- ShareFile.com/eu web servers designed to deliver the Web UI.
- API web servers used for client devices and tools using the HTTPS and REST API, including the Outlook plug-in, mobile and sync applications.
- Database – SQL database instances which contain things such as account data, file and folder metadata, including access rights, user account data, logs etc. The database in the SaaS Application tier does not process or store any customer data files.

The NetScalers and web servers are installed in the DMZ with the SQL databases installed in the private network behind an additional firewall. The SQL database instances are securely replicated to a second datacenter for backup and disaster recovery purposes.

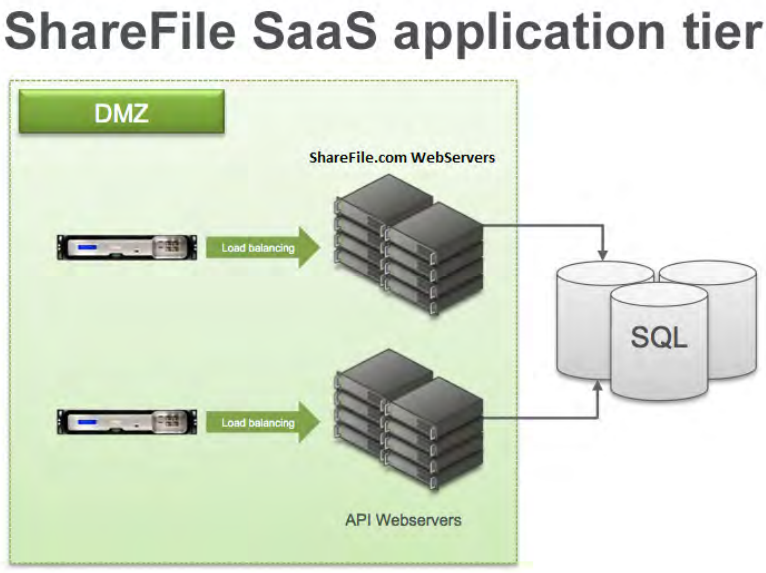

Figure 2: SaaS application tier components overview

SaaS application tier security

Encryption

To protect customer data in transit ShareFile supports SSL 3.0/TLS 1.0 with up to 256 bit AES encryption and no less than 128 bit encryption with the negotiation to TLS/AES-256 dependent on whether the end user's device or proxy supports TLS/AES-256.

Hash-based message authentication code

Hashing is defined as producing hash values for accessing data or for security purposes. A hash value (or simply hash) is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

In security systems, hashes are used to ensure that transmitted messages have not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If the hashes are the same, it indicates that the message was transmitted intact.

Metadata

Customer files are never processed, stored or transferred to the ShareFile SaaS application tier. Instead we store metadata which when defined means 'data about data' or data that describes other data. The metadata attributes that ShareFile stores in the SaaS application tier's database servers are as follows:

User info:

First name

Last name

User login (Email address)

Company name (Optional)

Password hash

Security question

Security answer

Access control lists (ACL)

File info:

File name

File description

File location

File size

File hash

File creation date

Email notification

Access control lists (ACL)

IP address from which file was uploaded

Other:

Account subdomains on ShareFile.com/eu

Audit & reporting

Citrix managed StorageZones

Overview

Citrix ShareFile operates a hybrid cloud infrastructure, with separate application and storage tiers managed by separate entities. Citrix manages the SaaS application tier (no file content) while an enterprise class cloud services provider (either Amazon Web Services or Microsoft Azure, depending on customer contract) hosts the StorageZone servers, along with application servers running the FTP/FTPS, Antivirus, Indexing, and Thumbnail services.

The Citrix managed StorageZones architecture consists of the SaaS Application tier, StorageZone Controller server(s) and cloud storage (see Figure 3).

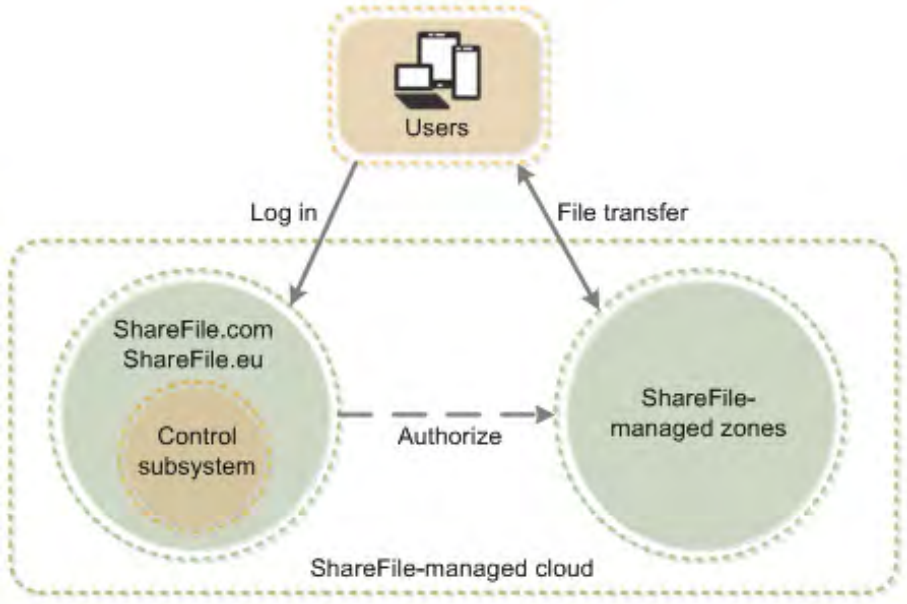

Figure 3: Citrix managed StorageZones architectural overview

Securing file upload/Download requests

When a user uploads or downloads a file, ShareFile's architecture prevents forged requests by using hash-based message authentication codes or HMAC's.

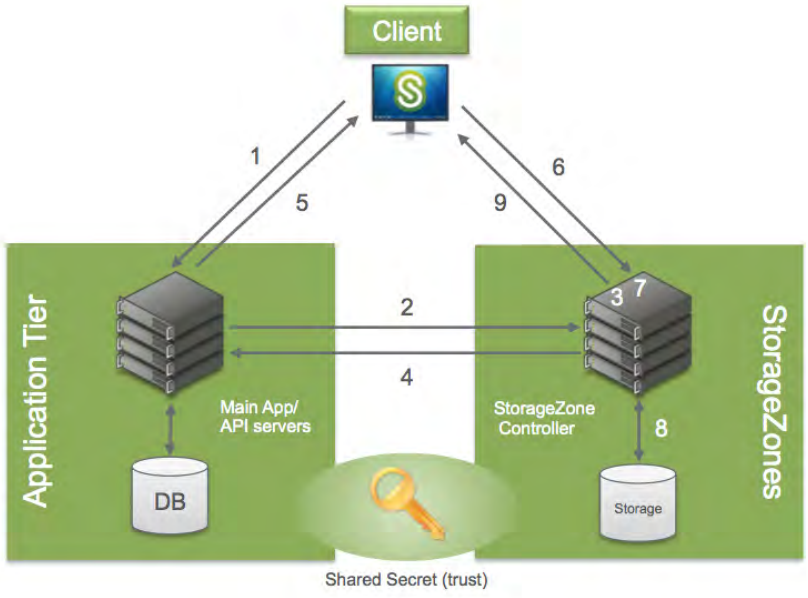

Figure 4: Preventing forged requests workflow diagram

1. Client requests a file.
2. A prepare message is sent by the ShareFile web application or API servers in the SaaS application tier to the StorageZone hosting the file. The location of the file is stored in the SaaS application tier database, accessed by the ShareFile web application and API servers.
3. A hash-based message authentication code (HMAC) based on the Shared Key used to establish a trust relationship between the SaaS application tier and StorageZone, is sent as part of the prepare message and is validated by the StorageZone Controller.
4. Once validated, the StorageZone confirms the validity and generates a unique one-time-use download token.
5. The ShareFile web application or API server provides the download link containing the fully qualified domain name (FQDN) of the StorageZones controller to the client with the unique download token.
6. To start the actual download, the client connects directly to the StorageZone.
7. The download token (part of the download request from the client), is validated.
8. If validation is successful, the file will be retrieved from storage, and the StorageZone will provide the file to the client.

Security

Encryption in transit

Client files are protected in transit between the web application and storage tier using SSL 3.0/TLS1.0 with no less than128 bit encryption depending on end-user browser configuration.

Encryption at rest

All client files are encrypted using AES 256-bit symmetric key encryption, a FIPS approved encryption algorithm.

Data backup

Customer files are stored redundantly within the cloud storage provider's region and ShareFile backs up all files daily. We store and back up customer files according to the data retention and version settings your dedicated ShareFile admin configures via the ShareFile administrative web interface.

Anti-virus

We employ dedicated antivirus servers that, based on customer preference, can scan all client files for malware. Any infected file is marked with a Red exclamation mark to warn end users of the risk associated with downloading an infected file.

Amazon Web Services security

The ShareFile infrastructure is segmented logically from other vendors using a concept Amazon Web Services refers to as Security Groups. Think of security groups as a firewall-like implementation that segregates ShareFile's infrastructure from other vendors.

Amazon EC2 provides a firewall solution to enable security groups; this mandatory inbound firewall is configured in a default deny mode and we must explicitly open any ports to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or CIDR block).

Amazon Web Services runs in geographically dispersed data centers that comply with key industry standards for security, reliability and confidentiality, such as ISO/IEC 27001:2005, SOC 1 and SOC 2.

Microsoft Azure security

Like Amazon Web Services, Windows Azure runs in geographically dispersed data centers that comply ISO/IEC 27001:2005, SOC 1 and SOC 2. Data centers are managed, monitored, and administered by Microsoft operations staff that have years of experience in delivering the world's largest online services with 24 x 7 continuity.

In addition to datacenter, network, and personnel security practices, Windows Azure incorporates security practices at the application and platform layers to enhance security for application developers and service administrators.

Customer managed StorageZones with on-prem storage
Overview

Customer managed StorageZones allow IT administrators to choose where corporate data will be processed and stored. IT can store data in the organization's data-center to help meet unique data sovereignty and compliance requirements, or an organization can choose to host ShareFile data natively in a Microsoft Azure account, helping IT build the most cost-effective and customized solution for their organization.

The on-premise customer-managed data can be easily integrated with an organization's existing infrastructure as it is designed to support any Common Internet File System (CIFS)-based network share. In both options the SaaS application tier is a required component.

The customer managed on-premise architecture consists of the SaaS Application tier, StorageZone Controller server(s) and customer datacenter hosted backend storage (see Figure 5.).

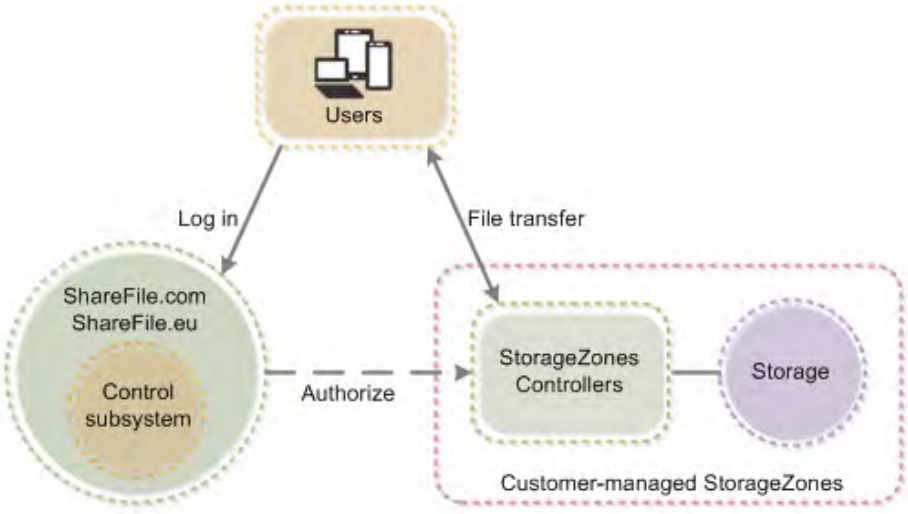

Figure 5: Customer managed on-premise StorageZones components diagram

Securing file upload/Download requests

The workflow is the same as Citrix managed StorageZones. The ShareFile architecture in customer managed StorageZones prevents forged upload and download requests by using hash-based message authentication codes (HMAC) as well.

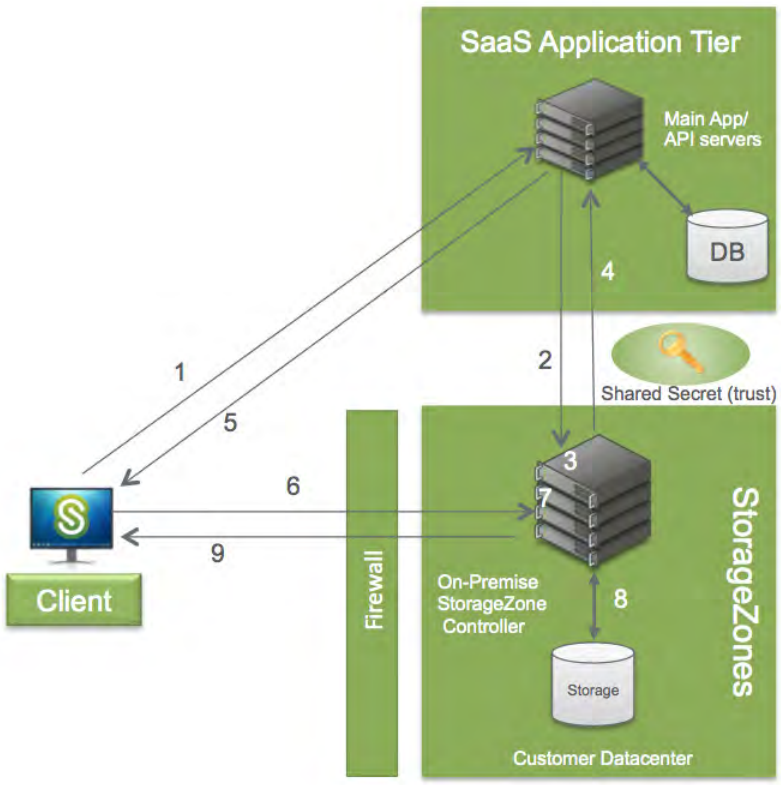

Figure 6: Preventing forged requests workflow diagram

1. Client requests a file.
2. A prepare message is sent by the ShareFile web application or API servers in the SaaS application tier to the StorageZone hosting the file. The location of the file is stored in the SaaS application tier database, accessed by the ShareFile web application and API servers.
3. A hash-based message authentication code (HMAC) based on the Shared Key used to establish a trust relation between the SaaS application tier and StorageZone, is sent as part of the prepare message and is validated by the StorageZone Controller.
4. Once validated, the StorageZone confirms the validity and generates a unique one-time-use download token.
5. The ShareFile web application or API server provides the download link to the Client with the unique download token.

6. To start the actual download, the Client connects to the StorageZone.

7. The download token (part of the download request from the Client), is validated.

8. If validation is successful, the file will be retrieved from storage.

9. The StorageZones controller server will send the file to the Client.

Security

Trust and encryption: On-premise StorageZone

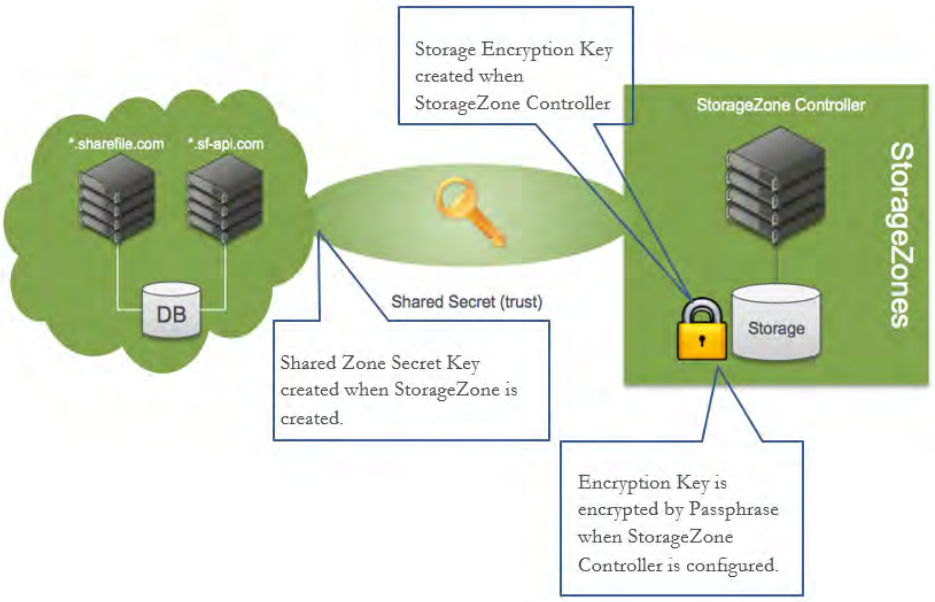

Figure 7: Security related SZ Controller configurations

ShareFile StorageZones controller server

Once the pre-requisites for installation are met, installing the StorageZones Controller server software is simple and consists of launching an .MSI file and clicking through until finished.

Pre-requisites:

- Use a publicly-resolvable Internet hostname (not an IP address).
- Install a commercially trusted SSL certificate in IIS.
- Allow inbound TCP requests on port 443 through the Windows firewall.

The installation file installs the following server components:

- A virtual directory and files into the IIS Default Web site. The physical location of the folder and files is c:\intetpub\wwwroot\Citrix\StorageCenter.
- An IIS application pool named StorageCenterAppPool. The installer also points the IIS Default Web Site's application pool to the newly created StorageCenterAppPool application pool.
- 4 windows services:
  - Citrix ShareFile Cloud Storage Uploader Service
  - Citrix ShareFile File Cleanup Service
  - Citrix ShareFile Copy Service
  - Citrix ShareFile Management Service

After installing the StorageZones Controller server software, configuration is required. Instructions on configuring the StorageZones Controller software can be found here. The configuration utility accomplishes the following tasks (see Figure 7):

- Creates a shared zone secret key in the customer's ShareFile account and on the StorageZones Controller server stored encrypted in the registry.
- Creates a storage encryption key (SCKeys.txt) and encrypts that key using 128 bit encryption when a passphrase is entered in the last step of the configuration. This encryption key is only used if the 'Enable Encryption' box is checked during configuration which instructs the StorageZone Controller server to encrypt the files stored in your shared ShareFile data repository.
- Creates a proprietary folder structure and the SCKeys.txt file in the ShareFile 'Storage Location' network share location defined during the configuration.
- Enables StorageZone Connectors if 'Enable StorageZone Connector for Network File Shares' and 'Enable StorageZone Connector for SharePoint' are checked. Enabling the Connectors creates the IIS apps "cifs" (Connector for Network File Shares) and "sp" (Connector for SharePoint)

Encryption in transit

If a NetScaler is not used in the architecture, customer files are protected in transit between the web application and the customer managed on-premise storage location using SSL 3.0/TLS1.0 with a minimum 128 bit encryption depending on end-user browser or proxy configuration

If customers are using Windows Azure, files are protected in transit between the web application and the customer managed on-premise storage location and to the Windows Azure storage container using the same SSL protocols as above.

If a NetScaler is used in the architecture, the SSL connection will be terminated at the NetScaler in the DMZ and files will be sent to the storage location either over http or https, depending on your configuration. If HTTP is used, files will traverse

the internal network to the storage location un-encrypted. If HTTPS is used, files will traverse the internal network to the storage location using SSL 3.0/TLS 1.0. The storage server will then decrypt the files and store them.

Encryption at rest

The StorageZones Controller software has the ability to encrypt the files located in the Storage Location defined during configuration. If data encryption is enabled, all zone files are encrypted with 128 bit encryption using the same key stored in SCKeys.txt. It is therefore critical that the SCKeys.txt file and passphrase be backed up to a secondary secure location. If the SCKeys.txt file is lost, all zone files become inaccessible. Because this directory resides in a customer managed datacenter it is a Citrix best practice to not have the StorageZones Controller software encrypt the data and leverage encryption options from your storage subsystem instead. If encrypted by the StorageZone Controller software, processes like anti-virus scanning and file indexing will not work.

If customers are using Windows Azure, the StorageZones Controller software has the ability to encrypt the files located in the temporary storage location defined during configuration. If the files are encrypted they will be transferred to the Windows Azure storage container encrypted. Decryption happens when a file is requested for download. The file gets copied from the Azure storage container to the temporary storage location in the customer datacenter where it is decrypted and sent from the StorageZones controller server to the client.

All communications from the StorageZones servers and Windows Azure storage containers happen over SSL.

Customer managed StorageZones with Windows Azure Storage

Overview

The Microsoft Azure customer-managed solution (Figure 8) integrates ShareFile with Microsoft Azure's Binary Large Object (Blob) storage, a cloud service for storing large amounts of unstructured data that can be accessed from anywhere in the world via HTTP or HTTPS.

The Azure Storage architecture is similar to the customer-managed on-premise StorageZones architecture with one minor difference. Azure storage is customer-managed storage hosted in the Azure cloud. File uploads are initially deposited into a temporary storage area shared by all StorageZone controllers. Then, a background service copies those files to the Windows Azure storage container and deletes the local cached copy of the file(s).

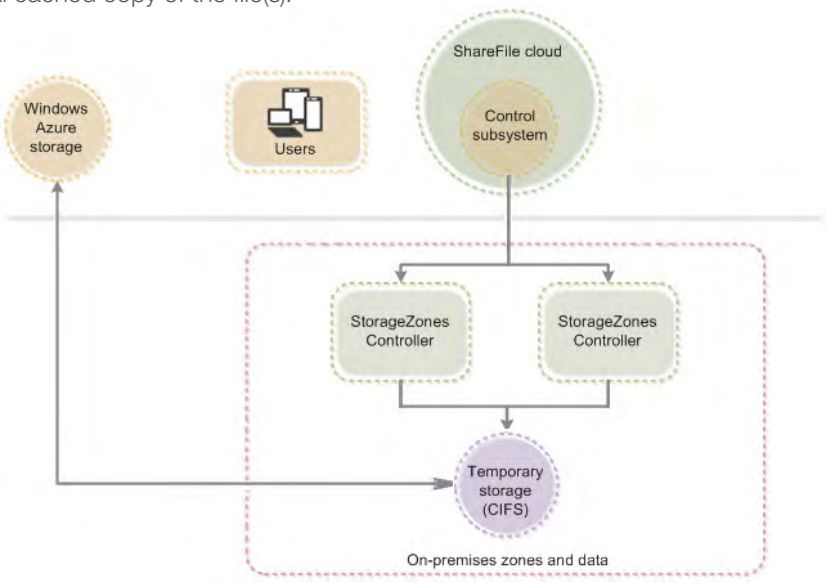

Figure 8: Customer managed StorageZones with Windows Azure components diagram

Securing file upload/Download requests

Because the architecture is very similar to the customer-managed on premise StorageZones architecture, the workflow is the same with one small difference highlighted in bold below.

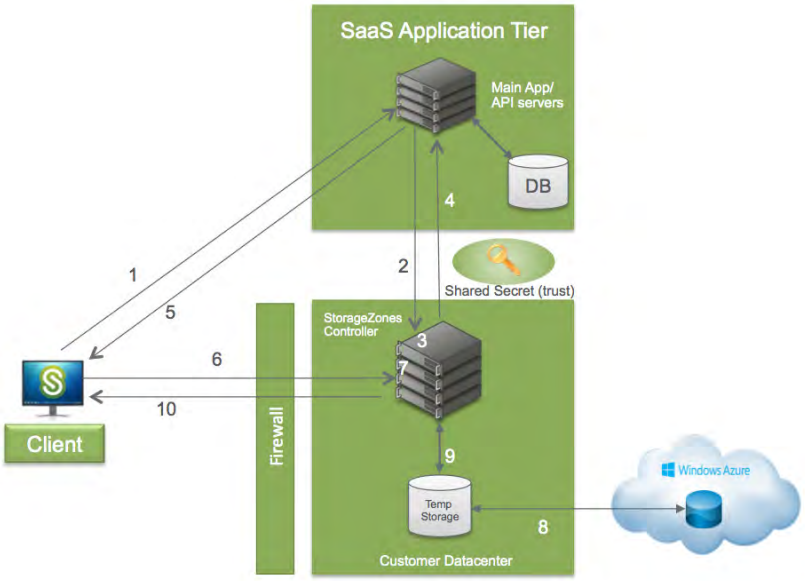

Figure 9: Preventing forged requests workflow diagram

1. Client requests a file.
2. A prepare message is sent by the ShareFile web application or API servers in the SaaS application tier to the StorageZone hosting the file. The location of the file is stored in the SaaS application tier database, accessed by the ShareFile web application and API servers.
3. A hash-based message authentication code (HMAC) based on the Shared Key used to establish a trust relation between the SaaS application tier and StorageZone, is sent as part of the prepare message and is validated by the StorageZone Controller.
4. Once validated, the StorageZone confirms the validity and generates a unique one-time-use download token.
5. The ShareFile web application or API server provides the download link to the Client with the unique download token.
6. To start the actual download, the Client connects to the StorageZone.
7. The download token (which is part of the download request from the Client), is validated.
8. If validation is successful, the file will be retrieved from Windows Azure storage and placed in the shared storage location in the customer datacenter.
9. The StorageZones controller server will send the file to the Client.

Security

The installation of the StorageZones controller software is identical to the customer managed on premise installation instructions, but the configuration of the software requires some additional steps.

Instructions on configuring the StorageZones Controller software with Windows Azure support can be found here and there is a video of the configuration located here. The configuration utility accomplishes the following tasks (see Figure 7 above) with the difference in configuration in bold below:

- Creates a shared zone secret key in the customer's ShareFile account and on the StorageZones Controller server stored encrypted in the registry.
- Creates a storage encryption key (SCKeys.txt) and encrypts that key using RC4 128 encryption when a passphrase is entered in the last step of the configuration. This encryption key is only used if the 'Enable Encryption' box is checked during configuration which instructs the StorageZone Controller server to encrypt the files stored in your shared ShareFile data repository.
- Creates a proprietary folder structure and the SCKeys.txt file in the ShareFile 'Storage Location' network share location defined during the configuration.

- Enables StorageZone Connectors if 'Enable StorageZone Connector for Network File Shares' and 'Enable StorageZone Connector for SharePoint' are checked. Enabling the Connectors creates the IIS apps "cifs" (Connector for Network File Shares) and "sp" (Connector for SharePoint).
- Connects the StorageZones controller server to the Windows Azure account using the account name and 512-bit authentication key generated in Azure when the Azure storage container is created. Once the StorageZones controller authenticates to Azure the administrator is presented with a list of available storage containers to choose from for the ShareFile data storage location.

StorageZone Connectors

Overview

ShareFile StorageZone Connectors, enabled by a customer managed implementation of a StorageZones controller server, help organizations leverage and mobilize existing enterprise data platforms. This feature, available in the ShareFile mobile app for iPhone, iPad and Android devices, allows mobile users to create a secure connection to existing CIFS network shares and SharePoint document libraries.

The StorageZone Connectors architecture consists of the SaaS application tier, a customer-managed implementation of a StorageZones Controller server, network shares and SharePoint document libraries.

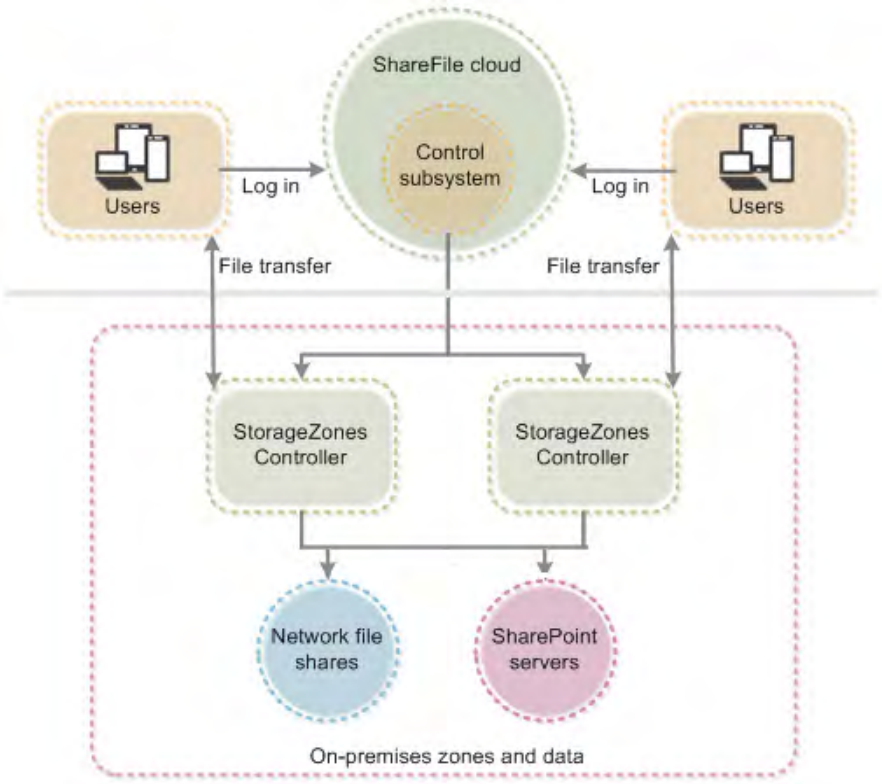

Figure 10: StorageZone Connectors component architecture

Securing file upload/Download requests

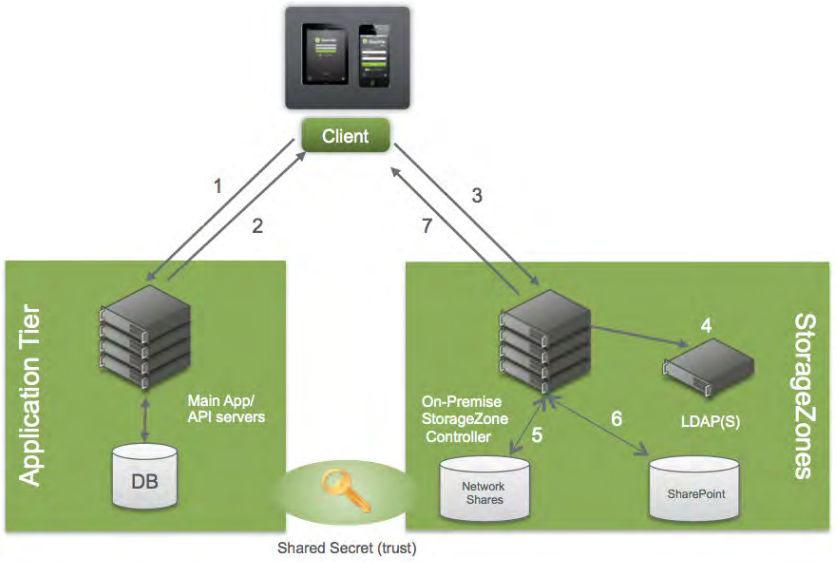

Figure 11: StorageZone Connectors workflow diagram without NetScaler

1. User login request sent to subdomain.sharefile.com
2. Top-level StorageZone connectors are displayed.
3. User login request sent to organizations Active Directory.
4. User authenticated to Active Directory.
5. Network shares enumeration.
6. SharePoint document libraries enumeration.
7. Files are uploaded/downloaded.

Security

When using StorageZone Connectors, an additional authentication step (Step 3 in Figure 10) is introduced when users access a Connector, and the file upload/download authorization step from sharefile.com is removed. Additional StorageZone Connectors security information:

- Clients always use HTTPS when initiating connections to the StorageZones Controller.
- HTTPS Basic authentication is required to support all mobile applications.
- Passwords are never sent in the clear by ShareFile clients.
- ShareFile administrators can control through user permissions which users have the ability to create connectors.
- Administrators can also whitelist/blacklist connectors to specific file shares and SharePoint libraries.

NetScaler integration

A demilitarized zone (DMZ) provides an extra layer of security for the internal network. A DMZ proxy, such as Citrix NetScaler VPX, is an optional component used to:

- Ensure all requests to a StorageZones originate from sharefile.com or sharefile.eu, so that only approved traffic reaches the StorageZone Controllers.
- Validates URI signatures before forwarding messages to StorageZone controllers reducing load on the StorageZone controllers.
- Load balance requests to StorageZone Controllers using real-time status indicators.
- Offload SSL from StorageZone Controllers.
- Ensure requests for files on SharePoint or network drives are authenticated before passing through the DMZ.

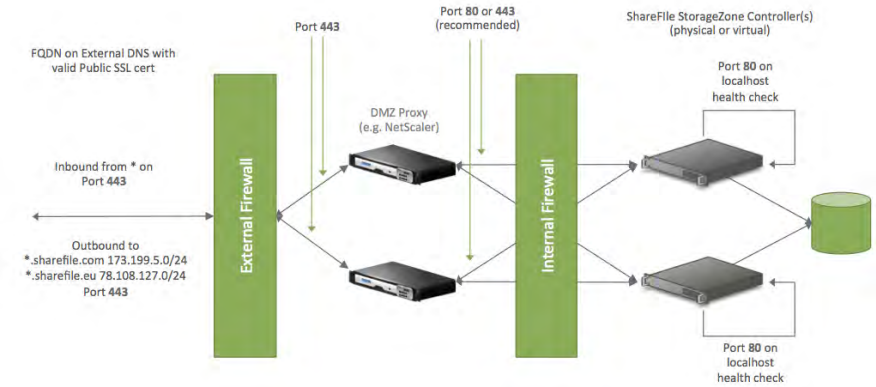

Figure 12: NetScaler components architecture for on-premise StorageZones Controllers

In this scenario, two firewalls stand between the Internet and the secure network. StorageZone Controllers reside in the internal network. User connections to ShareFile must traverse the first firewall and use the SSL protocol on port 443 to establish this connection. To support this connectivity, you must open port 443 on the firewall and install a public SSL certificate on the NetScaler appliances (if they terminate the user connection).

Overview

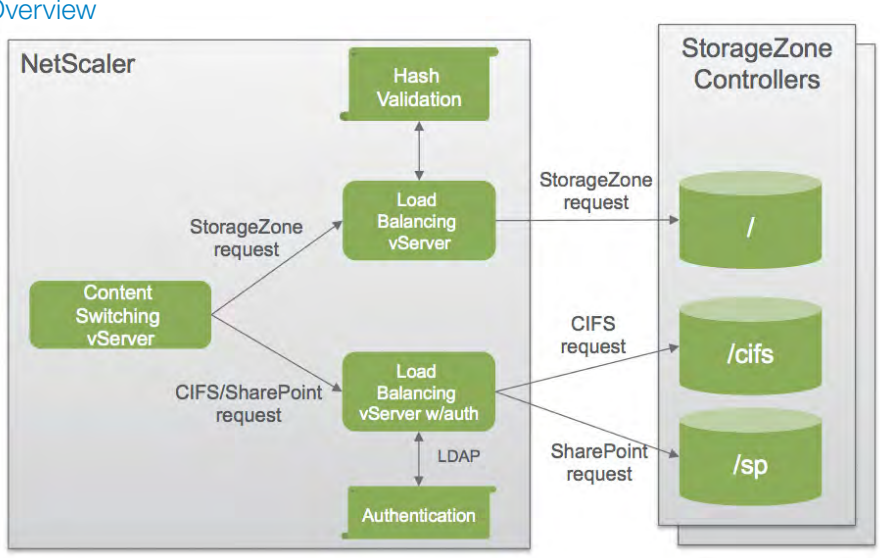

Figure 13: NetScaler configuration architectural diagram

- **NetScaler content switching virtual server** — sends user requests for data from ShareFile and from StorageZones Connectors to the appropriate NetScaler load balancing virtual server.
- **NetScaler load balancing virtual server** — Load balances the traffic for your StorageZones Controllers and also handles requests for data from your on-premise data storage and from StorageZone Connectors.

Requests for ShareFile data from on-premise data storage

A load balancing virtual server performs hash validation, to ensure valid URI signatures are present on incoming requests.

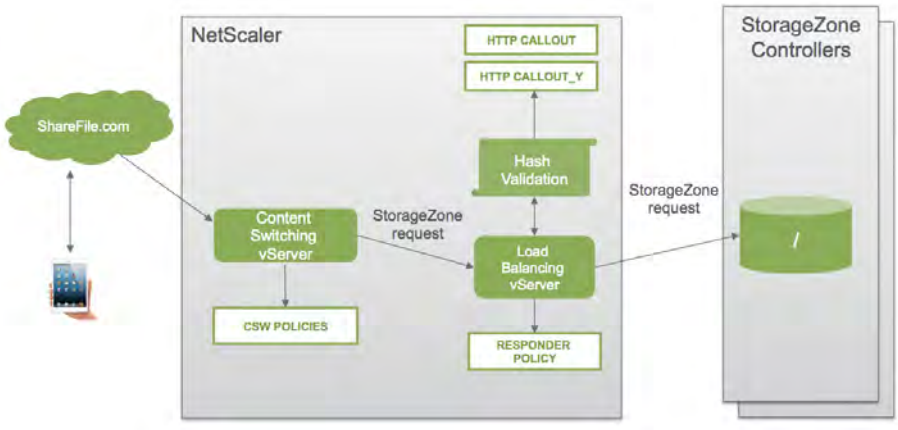

Figure 14: NetScaler configuration architectural diagram for ShareFile data

Securing ShareFile data upload/Download requests with NetScaler

The following diagram and table describe the network connections that occur when a user logs onto ShareFile and then downloads a document from an on-premise storage zone deployed behind NetScaler.

File activity is accessed via NetScaler in the DMZ, which terminates SSL, authenticates user requests and then accesses the StorageZone Controller in the trusted network on behalf of authenticated users. The NetScaler external address for ShareFile is accessed using the Internet FQDN szc.company.com (See Figure 15).

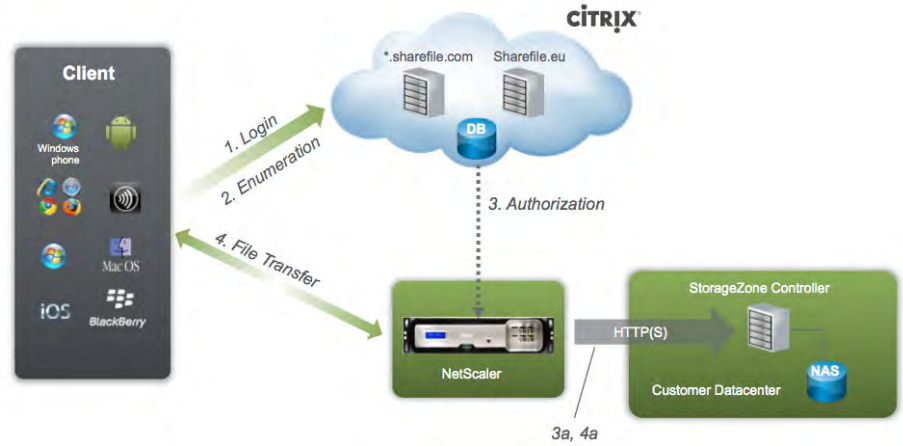

Figure 15: Securing requests for on-premise ShareFile data with NetScaler

1. The client makes a user logon request to company.sharefile.com over HTTPS.

2. The client makes a file/folder enumeration and download request to company.sharefile.com over HTTPS.

3. A file download authorization comes from sharefile.com to the szc.company.com (external address) over HTTP(S).

3a. A file download authorization is sent from the NetScaler NSIP to the StorageZones Controller over HTTPS

4. A file download request comes from the Client to the szc.company.com (external address) over HTTPS.

4a. A file download request is sent from the NetScaler NSIP to the StorageZones Controller server over HTTP(S).

5. The file is downloaded.

In between steps 4 and 5 the NetScaler strips the HMAC from the URI and sends the URI & HMAC to the StorageZones Controller server. The HMAC is validated by the StorageZones Controller server which then sends confirmation to NetScaler. The process completes and file is uploaded or downloaded.

Requests for data from StorageZones connectors

A load balancing virtual server performs user authentication. It stops a user request at the NetScaler, authenticates the user, and then performs single sign-on of the user to the StorageZones Controller.

Although authentication to NetScaler is optional, it is a recommended best practice.

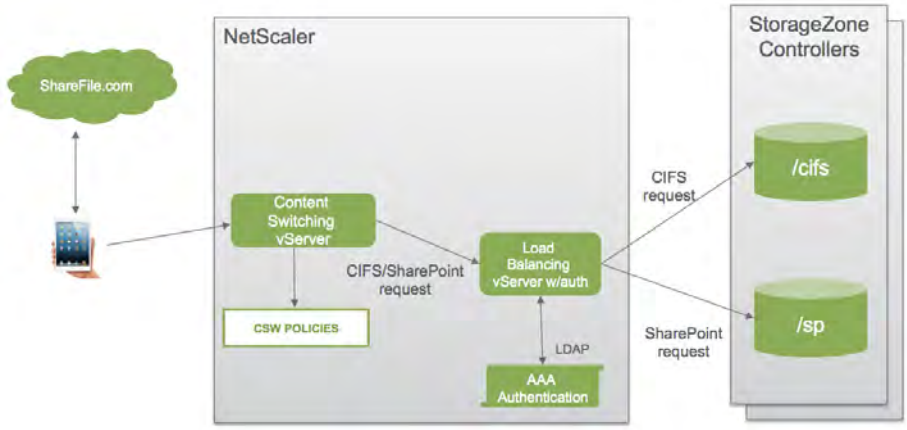

Figure 16: NetScaler configuration architectural diagram for StorageZone Connectors

Securing ShareFile Connector Upload/Download Requests with NetScaler

The following diagram and table extend the previous scenario (see Figure 15) to show the network connections for StorageZone Connectors. This scenario includes the use of NetScaler in the DMZ to terminate SSL and perform user authentication for Connectors access.

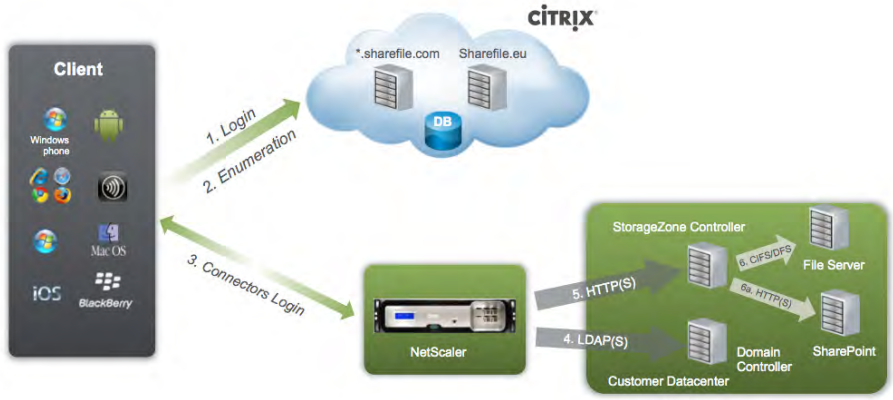

Figure 17: Securing requests for ShareFile Connector data with NetScaler

1. The client makes a user logon request to company.sharefile.com over HTTPS.
2. The client requests top-level connector enumeration from company.sharefile.com over HTTPS.

3. The client then sends a user logon to the StorageZones Controller server via the szc.company.com (external address) over HTTPS.
4. The user is authenticated from the NetScaler NSIP to the AD domain controller over LDAP(S).
5. The NetScaler NSIP sends file/folder enumeration and upload/download requests to the StorageZones Controller over HTTP(S).
6. The StorageZones Controller servers sends network share enumeration and upload/download requests to the customer file server over CIFS or DFS.

6a. The StorageZones Controller server sends SharePoint enumeration and upload/download requests to the internal customer SharePoint server over HTTP(S).

SAML integration

Overview

Security Assertion Markup Language (SAML) is a standard for exchanging authentication and authorization data between security domains. SAML is an XML-based protocol that uses security tokens to pass information about a principal (usually an end user) between a SAML authority, (an identity provider), and a SAML consumer, (a service provider). SAML enables web-based authentication and authorization scenarios including cross-domain single sign-on (SSO), which helps reduce the administrative overhead of distributing multiple authentication tokens to an end user.

Citrix ShareFile supports single sign-on via SAML 2.0 and integrates with a number of federated identity management solutions. ShareFile requires SAML assertions to include a NameID in the format emailAddress.

Workflow

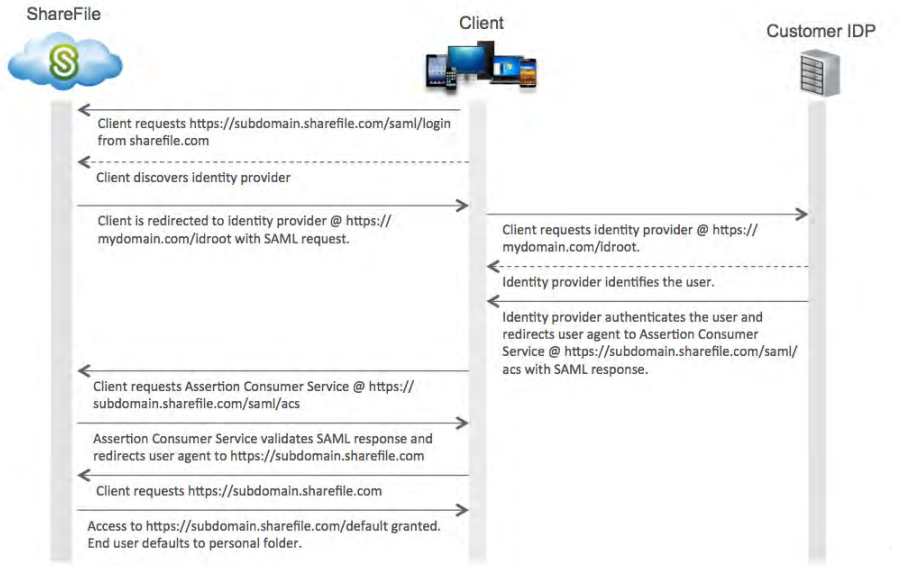

Figure 18: ShareFile SAML 2.0 Workflow

1. Client requests https://subdomain.sharefile.com/saml/login from sharefile.com
2. Client discovers identity provider.
3. Client is redirected via an HTTPS 302 redirect to identity provider @ https://mydomain.com/idroot with SAML request.
4. Client requests identity provider @ https://mydomain.com/idrood.
5. Identity provider authenticates the user and redirects client to Assertion Consumer Service @ https://subdomain.sharefile.com/saml/acs with SAML response.
6. Client posts SAML response to the Assertion Consumer Service @ https://subdomain.sharefile.com/saml/acs.
7. Assertion Consumer Service validates SAML response and authenticates the user if successful. ShareFile sets a session cookie and redirects Client to https://subdomain.sharefile.com.
8. Client requests https://subdomain.sharefile.com.
9. Access to https://subdomain.sharefile.com/default granted. End user defaults to personal folder.

Security and benefits

- User passwords never cross the firewall, since user authentication occurs inside of the firewall and multiple web application passwords are no longer required.
- Web applications with no passwords are virtually impossible to hack, as the user must authenticate against an enterprise-class Identity Provider first, which can include strong authentication mechanisms.
- "Service Provider (SP)-initiated" SAML SSO provides access to web apps for users outside of the firewall. If an outside user requests access to a web application, the SP can automatically redirect the user to an authentication portal located at the Identity Provider. After authenticating, the user is granted access to the application, while their login and password remains locked safely inside the firewall.
- Centralized federation provides a single point of web application access, control and auditing, which has security, risk and compliance benefits.
- The ability to offer secure, scalable, standards-based Internet SSO to customers, either as a value-added service, a competitive differentiator, or to satisfy customer demands.
- Ability to federate with other service providers, sharing user identity in order to deliver seamless, transparent, value-added services without requiring an additional login.

Additional resources

These additional resources can be used to get more information on ShareFile SAML configuration.

1. Configure Single Sign-on for SAML-Based Federation using ADFS
2. Configure Single Sign-on for SAML-Based Federation using Ping Federate
3. Configure Single Sign-on for SAML-Based Federation using CA SiteMinder
4. Configure Single Sign-on for SAML-Based Federation using OKTA

Conclusion

This paper details how ShareFile is secure by design, and enumerates the complete set of security and compliance controls available to ShareFile Enterprise customers.

- Flexible data storage – Organizations can selectively store ShareFile data in Citrix-managed StorageZones, which provide highly secure cloud storage without the need for on-premise infrastructure or maintenance; in StorageZones managed directly within the customer's own datacenter; or in both. This flexibility helps IT address the organization's unique data sovereignty and compliance requirements while building the most cost- effective and customized solution.
- Seamless integration with existing data platforms – Working in conjunction with customer-managed StorageZones, StorageZone Connectors let IT create a secure connection between the ShareFile service and user data stored in existing network shares without the need for data migration.
- Enterprise-grade security – ShareFile is an enterprise solution that provides extensive data protection features. Files are encrypted both at rest and in transit. Remote wipe allows secure destruction of all ShareFile-stored data and passwords on a device that has been compromised. IT can also remove a device from the list of devices that can access ShareFile accounts, or lock a device to restrict its use for a defined period of time. A poison pill capability lets IT prescribe data expiration policies for mobile devices.
- Auditing and reporting – IT can track and log all user activity, including both data access and data sharing, to support compliance requirements and provide visibility into data usage. Users and IT can also create custom reports on account usage and access.

Citrix ShareFile makes it possible for IT to provide the anywhere, any device data access and collaboration people need while meeting the organization's requirements for security, manageability and compliance. With more than two decades of experience serving enterprise IT, Citrix designed ShareFile as a true enterprise-class solution that eliminates the threat posed by consumer file sharing services while providing the industry's most comprehensive feature set. By making follow-me data a seamless and intuitive part of every user's day, ShareFile enables optimal productivity for today's highly mobile, anywhere, any device workforce.

Appendix A
Mobile security

This section summarizes the ShareFile security controls available for mobile devices. Many controls are provided as a native part of ShareFile. When ShareFile is used in conjunction with the XenMobile enterprise solution, more controls become available. The table below indicates which security controls are provided by ShareFile and XenMobile enterprise, and which are applicable to iOS or Android devices.

Security control	Description	iOS	Android
Provided by ShareFile			
Disable offline access	Allow or deny download of documents to the mobile device for offline viewing or editing When enabled, the user must be on the network to view or edit documents	✓	✓
Require password	Whether end users can save their password on the device. When disabled, users must authenticate each time the app is launched	✓	✓
File self-destruct	Documents downloaded to the device are automatically removed after a fixed amount of time	✓	✓
Encrypt files at rest	Device-specific file encryption within the ShareFile app—requires passcode lock setting to be enabled	✓	✓
Passcode lock	Prompts user for a ShareFile-specific passcode whenever the ShareFile app is launched	✓	✓
Device lock	Prevents user from logging onto the current account with the ShareFile app until the administrator unlocks the device	✓	✓
Jail-break detection	Prevent use of the ShareFile app if the device is jail-broken	✓	✓

Wipe	Removes all ShareFile account information and data from the device. Status of the wipe operation is communicated to the control plane. Applies only to ShareFile account data; see XenMobile and App-Controller sections for more comprehensive wipe options.	✓	✓
Wipe status and auditing	Status of the wipe request is communicated to the ShareFile administrator as pending or complete. After wipe completion, any actions performed by the client after the wipe was requested are reported to the administrator.	✓	✓
Disable external applications	Prevents opening of downloaded ShareFile documents in third-party apps ("open in")	✓	✓
Secure Sharing	Require recipients of shared files and folders to log on prior to download	✓	✓
Session inactivity timeout	Automatically log out inactive users after a configured amount of time	✓	✓
Provided by XenMobile			
Constrain clipboard cut and copy	Allow/disallow cut and copy of data from the ShareFile app to be pasted into other applications	✓	✓
Constrain clipboard paste	Allow/disallow data from other applications to be pasted into the ShareFile app	✓	
Constrain external applications	Allow/disallow only approved (MDX wrapped) external applications to be used for opening ShareFile documents (open in)	✓	✓
Constrain URL Schemes	Filter the URL schemes that are passed into the ShareFile application for handling	✓	✓

Block camera	Prevent ShareFile from using the device camera to upload photos or videos taken with the device	✓	✓
Block microphone	Prevent ShareFile from using the device microphone to capture and upload videos taken with the device	✓	✓
Block screen capture	Prevent a user-initiated screen capture operation while ShareFile is running		✓
Block email compose	Prevent ShareFile from sending e-mails via the native mail application	✓	
Disable print	Enable or disable printing of ShareFile documents from the mobile device to a network printer	✓	
Require Citrix Worx Home Authentication	The user must have a valid session with Worx Home in order to use ShareFile. A separate password can be required for offline access.	✓	✓
Define maximum offline period	Defines the maximum period ShareFile can run offline without a network logon	✓	✓
Require regular re-authentication	Challenge an authenticated user to re-authenticate at regular intervals in order to continue using ShareFile	✓	✓

Wipe data after security event	Any persistent data maintained by the ShareFile app can be erased, effectively resetting the app to its just installed state, if any of the following events occur: • Loss of app entitlement for the user • App subscription removed • Citrix Receiver account removed • Citrix Receiver uninstalled • Too many app authentication failures • Jail-broken or rooted device detected • Device placed in lock state by administrative action.	✓	✓
Online access only	The user must log on to Worx Home in order to use the ShareFile app—no offline access	✓	✓
Constrain WiFi networks	Require the device be connected to one of a white list of named WiFi networks in order to launch the app.	✓	✓
Require internal network	Require the device to be connected to an internal company network (determined by connectivity to an internal beacon)	✓	✓
Constrain network access	Require the ShareFile app to route all of its traffic through the company network	✓	✓
App update grace period	Defines the grace period during which users may use ShareFile after the system has discovered that a ShareFile app update is available. If set to 0, the update must be applied as soon as it becomes available.	✓	✓
Require device encryption	Locks the ShareFile app if the device does not have encryption configured	✓	✓

Require device pattern screen lock	Locks the ShareFile app if the device does not have a pattern screen lock configured		✓
Provided by XenMobile MDM			
Application white list/ black list	Allow or deny use of the ShareFile app on the device. If the application is installed before a black list policy is applied to the device, the app is removed.	✓	✓
Application provisioning	Install the ShareFile application automatically when the device is enrolled by XenMobile	✓	✓
Application removal	Remove the ShareFile application by administrator action or if the device is un-enrolled from XenMobile by the end user	✓	✓

Figure 19: Mobile Device Security table

Appendix B
ShareFile web application security features

The following ShareFile web application security and compliance features provides ShareFile the necessary tools to safeguard your data.

Features	Description
Configurable settings	
Password policy	Administrators have the option of configuring password policies including password history, expiration, and complexity controls such as length, uppercase and lowercase letters, at least one number, and at least one special character.
Custom SMTP (mail) settings	ShareFile enables accounts to route email messages through their own mail servers. When enabled, all e-mails sent through ShareFile will be routed through the client's mail sever, instead of ShareFile mail servers. Administrators may optionally configure the connection to support SSL.

SAML 2.0 enabled single sign-on	ShareFile supports SAML 2.0 for single sign-on and integrates with most SAML-compatible identity management solutions. (See section 7.) Accounts can be configured to allow a mix of SAML authentication and password-based authentication, or set to require SAML authentication for all users.
Multi-factor authentication	Administrators may set up a multi-factor (or strong) authentication process that requires submission of the account password and a secondary authentication, such as Google authentication or SMS/text message, in order to access the account. ShareFile supports various two-factor and two-step authentication methods including forms and token-based authentication as well as SMS, voice and backup codes.
File retention	Users can choose to automatically delete files a certain number of days after upload to support retention preferences and policies.
File versioning	Users can view different versions of a file uploaded with the same name to ensure that no changes are lost between updates or edits.
Terms and conditions	Terms and conditions can be displayed on the login page, with the option of including a check box on the login screen that must be marked to indicate compliance with the terms before logging in.
FTP/FTPS	By default, file transfers occur over HTTPS (Port 443). Optionally, users can connect to ShareFile using FTP or FTP over SSL (FTPS connection over port 990), an inherently more secure protocol than FTP. Users can connect to ShareFile directly from an FTP/FTPS program, providing a way for users to upload or download files to or from a secure location while using existing FTP/FTPS programs.
OAuth 2.0 support	ShareFile supports the OAuth authentication protocol with configurable OAuth token expiration time intervals.

Account lockout	ShareFile can configure your account to lock for five minutes after five invalid logon attempts to prevent account tampering. This application control is an account preference that can be customized to meet individual compliance needs.
Customized folder permissions	Administrative users can set folder permissions to ensure that employee and client users may only access specific folders. These permissions may be set to propagate to subfolders or apply only to specific subfolders.
Require login	ShareFile administrators can disable anonymous sharing requiring login for all file sharing.
Account activity reporting	ShareFile allows administrative users to run and access various reports on activity, usage, storage and permissions. Reports can be run on demand or emailed daily, weekly or monthly.
Email notifications	Users can choose to have customized notifications sent in real time or in a consolidated daily message.
Email domain whitelist / blacklist	ShareFile administrators can restrict file sharing based on email domain.
Access log retention	Detailed file-access logs are retained for at least one year.
File archiving	
Archiving for financial services	When enabled, ShareFile's archiving feature supports your compliance with federal regulations regarding data retention by retaining all files, links, attachments and versions either uploaded or sent through the ShareFile SMTP email server for a customizable period of at least three years.
ShareFile Cloud for Healthcare	
HIPAA	ShareFile provides multiple technical safeguards to support client compliance obligations under HIPAA. ShareFile supports your HIPAA compliance and will provide and sign a HIPAA Business Associate Agreement upon request.

Audit controls	Administrators can use the tools provided within ShareFile to review account activity, such as account usage and access to files and folders, to track disclosures.
Unique users and authentication	ShareFile provides administrators the capability to assign individual user accounts based on unique email addresses. Administrators are responsible for providing unique accounts and logins to each user.
Encryption	ShareFile handles the encryption and decryption of all files, including those presumed to contain PHI. Customers can, at their discretion, also encrypt files prior to uploading them to their ShareFile account.
Integrity controls	To help ensure that PHI has not been altered or destroyed in transit or at rest, ShareFile verifies file size and uses industry-accepted hashing algorithms to verify file integrity during file transfers.
Physical safeguards	Measures are in place to prevent unauthorized persons from gaining physical access to datacenters and systems, where PHI may be processed or stored. Infrastructure-as-a-Service providers do not have access to unencrypted customer files and do not manage encryption on Citrix's behalf.
Testing and evaluation	To maintain compliance with the HIPAA Security Rule, Citrix engages an independent third party to perform periodic risk assessments and gap analyses.

Figure 20: ShareFile web application security and compliance features table

Additional HIPAA documents can be located via the hyperlinks below.

What is the Citrix ShareFile Cloud for Healthcare?

Citrix ShareFile Cloud for Healthcare Frequently Asked Questions.

Corporate Headquarters
Fort Lauderdale, FL, USA

India Development Center
Bangalore, India

Latin America Headquarters
Coral Gables, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

Online Division Headquarters
Santa Barbara, CA, USA

UK Development Center
Chalfont, United Kingdom

EMEA Headquarters
Schaffhausen, Switzerland

Pacific Headquarters
Hong Kong, China

About Citrix
Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud infrastructure to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.