COMMVAULT®

Data Security

A COMMVAULT ENGINEERING WHITE PAPER

Enterprise security, governance and compliance is a major concern to most organizations, especially in this connected world where personal devices are used to access corporate data, which is frequently shared using free public file sharing services.

Commvault software provides comprehensive enterprise class security including full multi-tenancy support across all of its solutions such as enterprise data protection and recovery, end point protection, file sharing as well as data and application archiving, ensuring that your organization's data is secure, private and protected whether hosted on premise or in the cloud.

AUDIENCE

This white paper is intended for IT architects, administrators, Network administrators and security officers who are responsible for implementing or strengthening end to end data security. This document will help you understand the main security features incorporated into Commvault software and how they assist you in your data governance and compliance goals.

Contents

OVERVIEW

The first line of defense is always User security. Don't let unauthorized users gain physical access to your systems. In today's distributed world, that is increasingly more difficult.

Of course, hackers don't need to be in your data center to access your data. If copies of your data are available on remote devices such as laptops, the data is subject to loss or compromise. Organizations need the ability to locate, lock-down and wipe devices remotely. Endpoint Data security features are needed to protect remote data where it is entered, cached, and accessed by end users.

Remote connections may be essential to conduct your business, but they can also be entry points for hackers. Hackers may imitate or "spoof" a system to gain access through a network connection. Network security is essential to certify both authorized systems and users. Companies often use perimeter networks or Demilitarized Zone (DMZ) to prevent the exploitation of remote access points.

In some cases, your data may even be stored outside your physical data center for disaster recovery or long term retention. Providing Media security can prevent unauthorized access by other systems.

Portable media can be lost or stolen. You might even trust your data to third party vendors for off-site storage. In these cases, Data Encryption can help ensure that only authorized users can read the data.

USER SECURITY

ROLE BASED ACCESS CONTROL (RBAC)

Commvault software provides Role Based Access Control user security where a named role is used to define a discrete set of permissions. An administrator can assign roles to an Active Directory, Domino Directory Service, LDAP or an internally defined user or user group.

Multiple roles can be assigned to the same user or user group. Users can have roles assigned individually or inherited through user group membership.

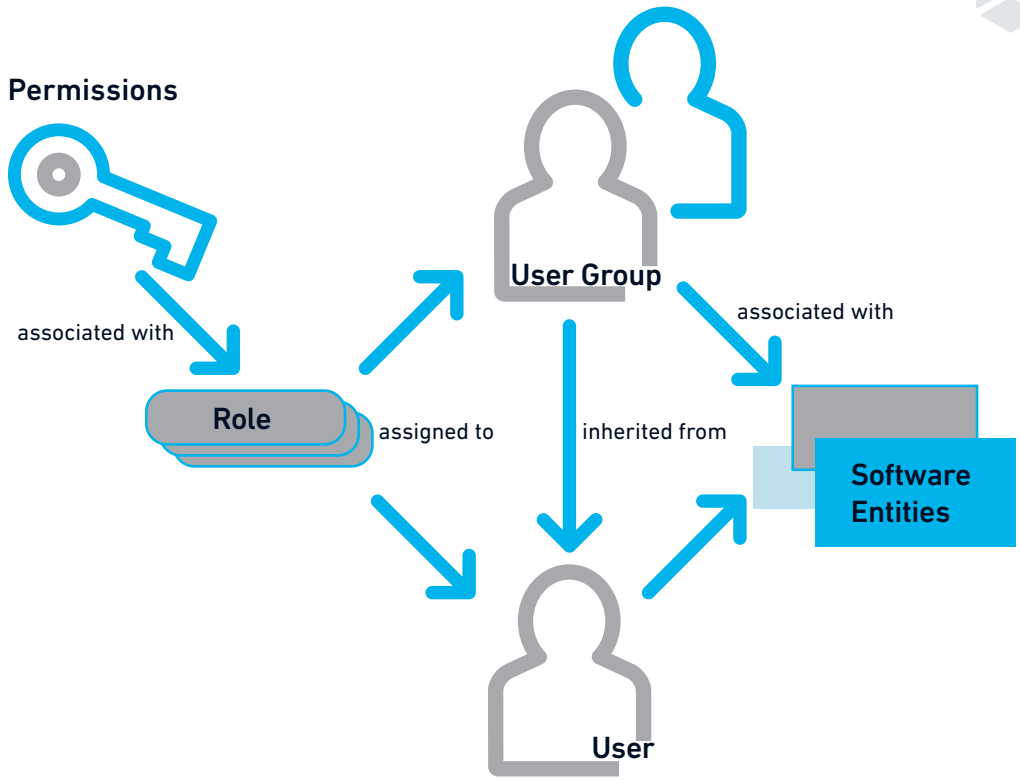


Figure 1: Example of Role, User, Entity Security Relationship

Each time a role is assigned to a user or user group it is associated with one or more software entities. Tasks authorized by a role assigned to a user can be performed by the user on those entities. Implementing role-based access control increases the flexibility of user security by enabling the administrator to align task authorization to business needs rather than to technology considerations. For multi-tenant environments or administrators who want to implement task distribution, RBAC provides a high degree of security granularity in providing users only those permissions necessary to perform the specified tasks on the data or components assigned.

Implementing role-based access control increases the flexibility of user security by enabling the administrator to align task authorization to business needs rather than to technology considerations.

For multi-tenant environments or administrators who want to implement task distribution, RBAC provides a high degree of security granularity in providing users only those permissions necessary to perform the specified tasks on the data or components assigned.

AUDITING AND SESSION MANAGEMENT

With the Audit Trail feature you can track every user's data access and software actions. Various levels of operations, such as Critical, High, Medium, and Low can be tracked and reported over time.

Administrators can also view session activity by real-time monitoring or user log on/log off activity. Inactive users can be disconnected immediately or automatically by activity timeout.

Audit reports and alerts can be configured to monitor and flag unauthorized login attempts and attempts to view or destroy data.

SECURITY INFORMATION AND EVENT MANAGEMENT

Commvault software provides a Log Monitoring tool that can monitor system events, user operations, logs, and analytic information for trend analysis and automated, centralized reporting as may be required for compliance. Auditors and administrators can customize what, where, and how often information is collected. They can monitor the results from a single point of view making it easier to spot trends and see patterns that are out of the ordinary.

INTEGRATION WITH MICROSOFT ACTIVE DIRECTORY AND IBM DOMINO DIRECTORY SERVICES

Companies exert a lot of effort in designing and maintaining their own user security architecture. Microsoft Active Directory, IBM Domino Directory services, and open sourced Lightweight Directory Access Protocol (LDAP) are trusted external authorities used for two purposes:

- Authenticate an external user.
- Validate a external user's access rights to search or browse data in protected storage.

Integration with external directory services allows an administrator to manage a single set of users. The administrator can assign roles and managed entities a directory service user or user group. Adding or disabling users becomes a single-step operation.

TWO-FACTOR AUTHENTICATION

Passwords alone might not provide enough security to protect your CommCell from unauthorized access. You can add an extra level of security to the CommCell logon requirements with Two-Factor Authentication.

When Two-Factor Authentication is activated, users must enter a 6-digit PIN (Personal Identification Number) along with their passwords to access the software interface. Administrators can provide users with a unique PIN to use for logon by any of the following methods:

- Registered email account
- Mobile apps
- Desktop application

Two-Factor Authentication can prevent an unauthorized person from accessing CommCell functions with a compromised password.

INTEGRATION WITH A SOCIAL MEDIA PROVIDER

Users who log on to the Web Console can be authenticated by a social media provider, for example, a user can log on by using credentials from a Google account.

OAuth is the authorization framework that performs the single sign-on (SSO) exchange with the social media provider. A workflow is used to validate the user identity then create and register the user in the software. All user activity including creation, registration, and all tasks performed are recorded and available through the software's user auditing capability.

SUPPORT FOR SECURITY ASSERTION MARKUP LANGUAGE (SAML)

SAML is an XML-based open standard that allows authentication by an Identity Provider (IdP) for users accessing data from a web browser. This allows organizations to provide secure yet easy access to data from their devices.

Some companies employ SAML to facilitate the use of a single identity for a one-time, SSO login for each user, for all applications. Commvault software provides a pre-defined SAML User Registration Workflow to create and register SAML connected users.

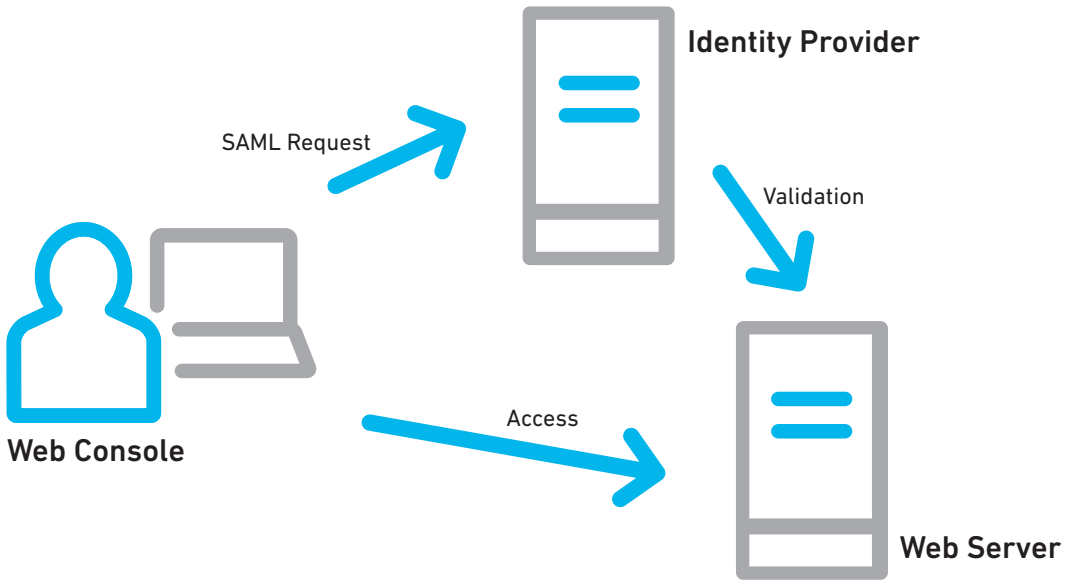


Figure 2: SAML Authentication Flow

ENDPOINT DATA SECURITY

SECURE FILE SHARING

Authorized end users can access their protected files and emails in protected storage by using remote devices such as smart phones, tablets or laptops.

Protected data belonging to a user can be shared with other users. Administrators can set permission levels (view or edit) so that these additional users can browse, download, or even upload files from a user's protected storage

PRIVACY AND CLIENT LOCKING

Client locking prevents unauthorized access to a lost or compromised client's protected data. A locked client requires a user to enter a password for the following tasks:

- Browse backup data
- Find data in protected storage
- Restore data from protected storage
- Add content for backup

Additionally, searches initiated from the Web Console or Compliance Search will skip locked client data in their search.

A good use of Client Locking is in a multi-tenant environment where administrative level access may be controlled by a 3rd party.

Commvault software's Privacy feature also enables a client owner to prevent IT or cloud administrators from viewing client data.

DATA LOSS PREVENTION

Data Loss Prevention (DLP) is a laptop security solution that can be seamlessly integrated into your operating system with the Explorer Plug-in for Windows laptops or the Finder Plug-In for Macintosh laptops.

With DLP, you can schedule periodic encryption of your document files on your device and, if your laptop is lost or stolen, prevent unauthorized access to your data. DLP secured content can be opened only by using the correct **Personal Data Loss Prevention Pass-key.** If an unauthorized user attempts to open a locked file, only scrambled, useless data appears.

If your laptop is ever lost or stolen, you can use DLP to protect sensitive data. Geo location can be used to help you find the laptop before erasing data. If the laptop is lost, you can use Secure Erase feature to erase certain files under the following circumstances:

- If the lost laptop has been offline without network connectivity for a specified number of days.
- If the lost laptop is turned on and connects with the network.

ERASE DATA

The Erase Data feature allows you to permanently erase any data from protected storage copied to it by a backup or archive operation. Erasure of data in protected storage may be necessary to meet compliance requirements or to remove all or an inadvertent copy of the original data. Using Erase Data, you can erase folders, files, mailboxes, folders in a mailbox, messages within a folder, and attachments.

NETWORK SECURITY

ENCRYPTED CHALLENGE AND REPLY

All network communications between Commvault software components use encrypted challenge and reply to validate the components involved. The CommServe host encrypts a challenge using the client's public key. In turn, the client decrypts the challenge by using its private key and sends an encrypted reply using the destination component's public key. Only after the destination component has successfully decrypted the client's reply by using its private key, is communication allowed to proceed.

CLIENT CERTIFICATES

Client certificates are used to authenticate connections between systems. The authentication process reveals and confirms the identity of the client attempting to establish connections during installation. Commvault software's certificate services are flexible and offer a number of implementation options:

Automatic Certificate assignment	This "locks down" each client and avoids third-party connections that do not have valid certificates.
Installation Certificate assignment	This action "locks down" installation attempts by denying client installations attempts which do not have valid per-client certificates.
Firewall Certificate assignment	This action "locks down" only those clients who communicate with the CommServe through a firewall proxy client.

In the event a client is lost or compromised, certificates can be revoked to deny further communication with other components.

FIREWALL

A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not secure and trusted. Administrators can allow trusted applications or hosts to communicate through a firewall.

Commvault software components separated by a firewall can be configured to use authorized ports and connection routes (inbound, outbound, two-way) through the firewall to communicate and perform data management operations such as backup, browse, restore, etc.

It's important to note that Commvault software's firewall access feature is not a firewall. Software or hardware firewalls must be configured to enable access ports and connection routes that allow software components to communicate through the firewall. The firewall feature enables the Administrator to configure a software component to use those authorized firewall ports and connection routes.

Commvault software firewall access feature supports four common firewall scenarios. These scenarios, or any combination of them, can be configured by using firewall access configuration tools.

SCENARIO 1: DIRECT CONNECTIONS USING PORT TUNNELS

Direct connection with port restrictions is a setup in which at least one of any two communicating computers can establish a one-to-one connection with the other on specific ports. The connection route must not include a proxy or an intermediate port-forwarding gateway. Three types of direct connections are supported:

- Client connects to the CommServe host or MediaAgent (one-way firewall inbound)
- CommServe host or MediaAgent connects to the client (one-way firewall outbound)
- Client and CommServe host or MediaAgent connect to each other (two-way firewall) These connections assume that the CommServe host or MediaAgent are in the secure, trusted network protected by the firewall.

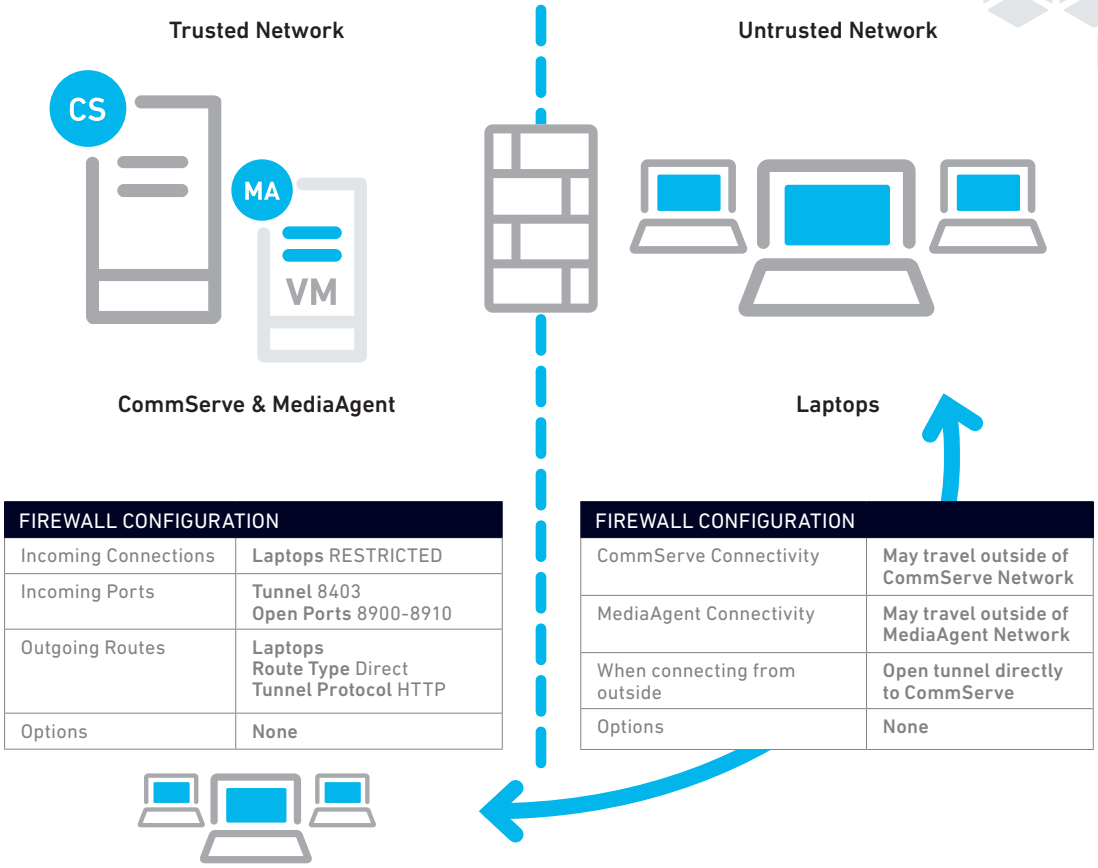


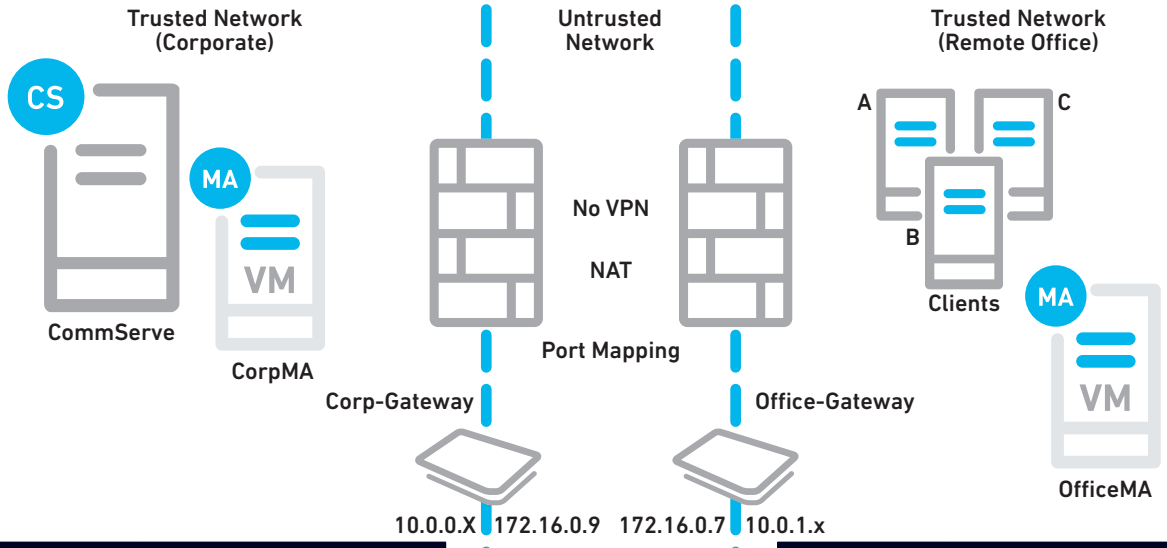
Figure 3: Example of Direct Connection Firewall Configuration

Figure 3 depicts a common "direction connection" firewall configuration. Clients within the "Laptops" client computer group can operate both inside and outside the firewall. Laptops are restricted to using the 8403 tunnel port to communicate with the CommServe host and open ports 8900-8910 for running data management jobs. All other clients are not affected by the firewall restrictions.

SCENARIO 2: PORT-FORWARDING GATEWAYS

A port-forwarding gateway is a firewall router configured to handle Network Address Translation (NAT) traffic. Hosts in a private or trusted network communicate with the public or untrusted network by using a common network IP address. Communication between public and private hosts that use a single public IP address is managed by assigning a unique port number to each host/service. For example: The CVD service in a private network of 10.0.0.x:8403 may be assigned (mapped) to a public address and port number of 172.16.0.7:9250. All private hosts listening on port 8403 will hear public traffic sent to 172.16.0.7:9250. The destination host will be encapsulated in the port-forwarded traffic.

Figure 4 depicts a common "gateway" firewall configuration. Trusted networks use private IP addresses to communicate within their trusted environment. Communication between the trusted networks over an untrusted network, use a single public IP address. Data traffic between hosts across the untrusted network is port-forwarded by the gateway routers.



FIREWALL CONFIGURATION	
Incoming Connections	**Clients** RESTRICTED **OfficeMA** RESTRICTED
Incoming Ports	**Tunnel** 8403
Outgoing Routes	**Client A** **Route Type** Via Gateway **GW Hostname** Corp-Gateway **GW TunnelPort** 8410 **Client B** **Route Type** Via Gateway **GW Hostname** Corp-Gateway **GW TunnelPort** 8411 **Client C** **Route Type** Via Gateway **GW Hostname** Corp-Gateway **GW TunnelPort** 8412 **OfficeMA** **Route Type** Via Gateway **GW Hostname** Corp-Gateway **GW TunnelPort** 8413
Options	**None**

Clients use local office MediaAgent. Office MediaAgent copies data to corporate MediaAgent

FIREWALL CONFIGURATION	
Incoming Connections	
Incoming Ports	**Tunnel** 8403
Outgoing Routes	**CommServe** **Route Type** Via Gateway **GW Hostname** Office-Gateway **GW TunnelPort** 8413 **CorpMA** **Route Type** Via Gateway **GW Hostname** Office-Gateway **GW TunnelPort** 8414
Options	**None**

Figure 4: Example of Port-forwarding Gateway Firewall Configuration

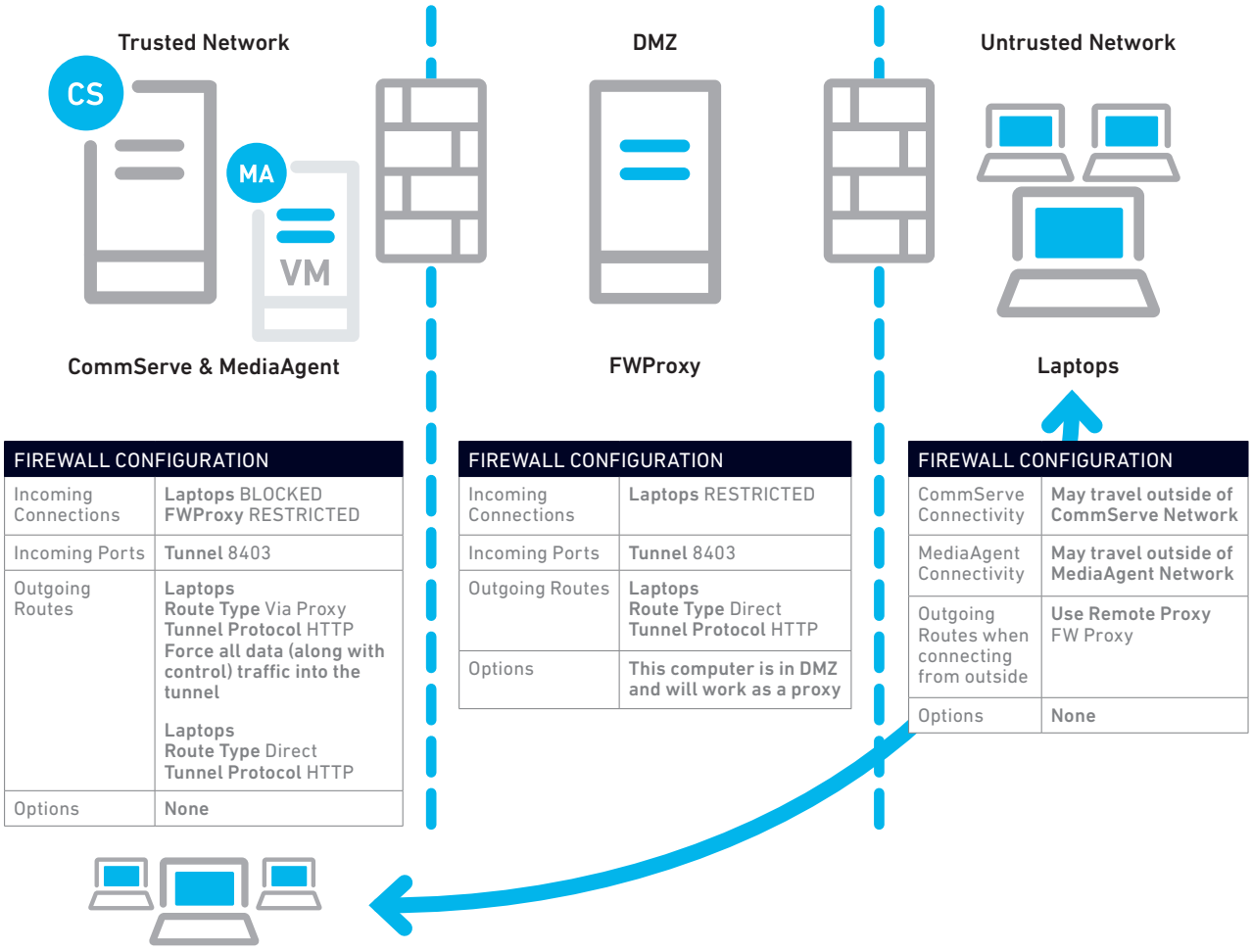
Remote office connections in which there are multiple systems are best served by using a Virtual Private Network (VPN). Without a VPN, each client must be individually addressed in the firewall configuration for port-forwarding.

SCENARIO 3: PERIMETER NETWORK USING A FIREWALL PROXY

A perimeter network or Demilitarized Zone (DMZ) is a physical or logical sub network that contains and exposes an organization's external-facing services to untrusted networks. The perimeter network adds an additional layer of security to a trusted network. An external attacker has direct

access to equipment only in the perimeter network, rather than any other part of the trusted network.

Figure 5 depicts a common perimeter network firewall configuration. Clients within the "Laptops" client computer group can operate both inside and outside the firewall. A firewall proxy is configured to operate within the perimeter network to forward traffic between the trusted network and untrusted network. Clients in the Laptops client computer group can roam inside and outside of the trusted network. This is why the outgoing routes have two routes for laptops.



FIREWALL CONFIGURATION	
Incoming Connections	**Laptops** BLOCKED **FWProxy** RESTRICTED
Incoming Ports	**Tunnel** 8403
Outgoing Routes	**Laptops** **Route Type** Via Proxy **Tunnel Protocol** HTTP **Force all data (along with control) traffic into the tunnel** **Laptops** **Route Type** Direct **Tunnel Protocol** HTTP
Options	**None**

FIREWALL CONFIGURATION	
Incoming Connections	**Laptops** RESTRICTED
Incoming Ports	**Tunnel** 8403
Outgoing Routes	**Laptops** **Route Type** Direct **Tunnel Protocol** HTTP
Options	**This computer is in DMZ and will work as a proxy**

FIREWALL CONFIGURATION	
CommServe Connectivity	**May travel outside of CommServe Network**
MediaAgent Connectivity	**May travel outside of MediaAgent Network**
Outgoing Routes when connecting from outside	**Use Remote Proxy** FW Proxy
Options	**None**

Figure 5: Example of Perimeter Network (DMZ) Using a Firewall Proxy Configuration

SCENARIO 4: HTTP PROXIES (WIFI CONNECTIONS)

Traveling users often have to operate in public locations such as a coffee shop, airport, or hotel where internet access requires going through an HTTP proxy. In this scenario, Commvault software is flexible and can support the proxy requirement for that user profile.

THIRD PARTY PORT MAPPING (TPPM)

In addition to the firewall routes configured in your CommCell setup, you can also establish connectivity between CommCell computers on third-party ports using existing firewall tunnels. These ports are used by third-party applications and are not configured with Commvault firewall access feature.

The Third-Party Port Mapping configuration allows you to set up a port on the destination computer and map it to a local port on the source computer to listen for incoming connections. This configuration is also referred to as port forwarding.

MEDIA SECURITY

MEDIA PASSWORD

The media password is used to prevent unauthorized access to non-encrypted data residing on removable media when using external recovery tools to restore data. This ensures that only the originating, licensed software can recover data written by that software.

For more granular security, you can even specify a different media password for different data content. For example you might have financial data or HR data. Having the ability to assign different media passwords enables compartmentalization so compromising of one password does not expose all data.

DATA ENCRYPTION

SOFTWARE

Commvault software supports encryption of data in transit (source to media) and data at rest (on media).

For data encryption in transit, the location of where the encryption takes place is flexible. If the transit path is vulnerable, encryption can take place at the source. If the target storage is secure, you can enable data encryption for the network only.

For offline data encryption, you can configure/enable encryption only on those media copies that require it. For example, you send a copy of the data offsite to a cloud provider or secure storage site.

For disk target storage with deduplication or compression enabled, encryption is performed after both have completed to allow either operation to reach its full benefit.

Commvault software offers a selection of encryption ciphers and key lengths including the Advanced Encryption Standard (AES) cipher. The crypto library module approved by the Federal Information Processing Standard (FIPS) supports data encryption ciphers recommended by FIPS, as well as additional commonly used data encryption ciphers.

The National Institute of Standards and Technology includes Commvault software in its list of Validated FIPS 140-1 and FIPS 140-2 cryptographic modules that have been tested by using the cryptographic module validation program.

HARDWARE

Tape devices such as LTO4 support encryption of data on the tape drive itself. Supported encryption-enabled tape drives are those that provide the necessary controls to the Commvault software to get the encryption capabilities and set the encryption properties on the drive.

You can also use inline hardware encryption devices with their own key management software such as Network Appliances (formerly Decru's) Datafort. These inline devices are transparent to the Commvault software data flow. However, data written through these devices must also be restored through these devices.

KEY MANAGEMENT

Key management is the ability to generate random encryption keys for the encryption cipher and manage the secure storage of these keys. Commvault software provides key management services for its software encryption ciphers and for supported encryption-enabled hardware devices.

Encryption keys are stored by using the AES Key Wrap. Because IDs are not embedded in the keys, the keys are identified by their storage location in the database. Encryption keys can optionally be stored on the media itself for offline recovery.

Commvault software encryption keys are generated by using an ANSI 9.31 random number generator. ANSI 9.31 is the standard for digital signatures based on the RSA algorithm. It uses the MDC-2 hash algorithm to produce an RSA key pair for the client, generate random 128-bit or 256-bit data encryption keys for every chunk, and create initialization vectors for Cypher Block Chaining during data encryption.

Commvault software generates a different random 128 or 256 key for every chunk of data written. Each job can contain multiple chunks, so each backup job can have multiple randomly generated keys. With multiple different keys the strength of the encryption is high. You can provide additional protection for Commvault software encryption keys with the use of **SafeNet** before storing the keys in the software database. During software encryption, the encryption key is encrypted with a public key that can be decrypted only with a private key. You can encrypt the private key and store it on the SafeNet server. SafeNet keys are required for restore and auxiliary copy operations.

SUMMARY

Data protection is the highest priority for Commvault. It's the definition of our business and service to our customers. We have built in security at every step of our data management services. By using our security features and tools to augment and enhance your own data security plan, you will ensure that your data is kept private and safe from unauthorized users.

COMMVAULT®

PROTECT. ACCESS. COMPLY. SHARE.

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM