FORTRA

Globalscape EFT System Architecture Guide

Copyright Terms and Conditions

202310251153

Table of Contents

Introduction

Globalscape EFT is a managed file transfer solution that streamlines the exchange of data between your systems, employees, customers, and trading partners. It provides a single point of control with extensive security settings, workflow management, detailed audit trails, and reports.

The intuitive EFT interface and comprehensive workflow features help to eliminate the need for custom programs/scripts, single-function tools, and manual processes. This innovative solution reduces costs, improves the quality of your file transfers, and helps your organization comply with data security policies and regulations.

EFT can be installed as a standalone deployment with one server (which can have multiple sites/IP addresses) or in a variety of more complex options, including cloud deployments, depending on what you need to accomplish.

With integrated support for clustering, EFT can process high volumes of file transfers for enterprises by load balancing processes across multiple nodes. The clustering technology in EFT also provides active-active automatic failover for disaster recovery.

EFT can be scaled horizontally by adding additional systems to the cluster. When paired with a load balancer, inbound connections to file servers can be distributed to the available systems in the cluster. As your business and transfer requirements grow, EFT can easily grow with it by adding additional servers to the cluster.

This guide includes several EFT different architectures, including support for high availability (clustering) and load balancing, and summarizes the advantages of each configuration.

Standalone EFT Server

In this architecture, a single EFT server instance is installed behind the front-end firewall. If file transfer services are enabled, ports to the HTTP/S, FTP, FTPS, SFTP, and AS2 protocols are opened on the firewall to allow all inbound connections to EFT.

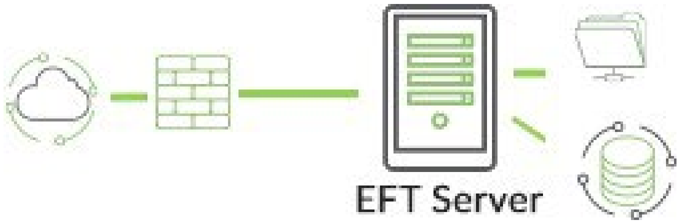


Figure 1 Standalone EFT Server

The default standalone system uses the installed EFT database files for configuration, and (optionally) SQL or Oracle database inside the private network for storing auditing and reporting data. EFT includes an automated backup and cleanup event rule in case of application failure. EFT includes automated backup and cleanup event rules in case of application failure.

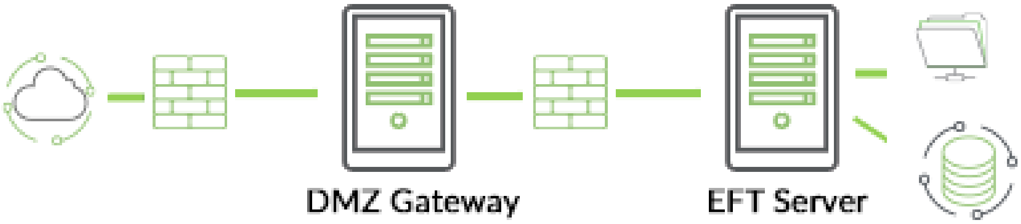


Figure 2 Standalone EFT Server with DMZ Gateway

An optional DMZ Gateway® can be installed in the demilitarized zone (DMZ) to provide secure communication with EFT behind intranet firewalls without requiring any inbound firewall holes between the internal network and the DMZ.

Requisites

- 1 EFT
- Database server (optional)
- 1 DMZ (optional)

Benefits

- Ideal for small organization where high availability is not needed

Development and Test

Globalscape recommends having an environment for development and/or testing purposes, which requires an additional EFT non-production license. This extra license is helpful for providing change control and quality assurance of new workflows that you build in EFT. It will also allow you to test new releases/patches in an isolated environment.

EFT allows authorized administrative users to export workflows, schedules, and other items from a development/test environment and import them into production. EFT server and site configuration, stored in .db files, can be exported and imported using a tool such as SQLite.

Load testing is recommended in staging environments for definitive settings that meet your organization's requirements.

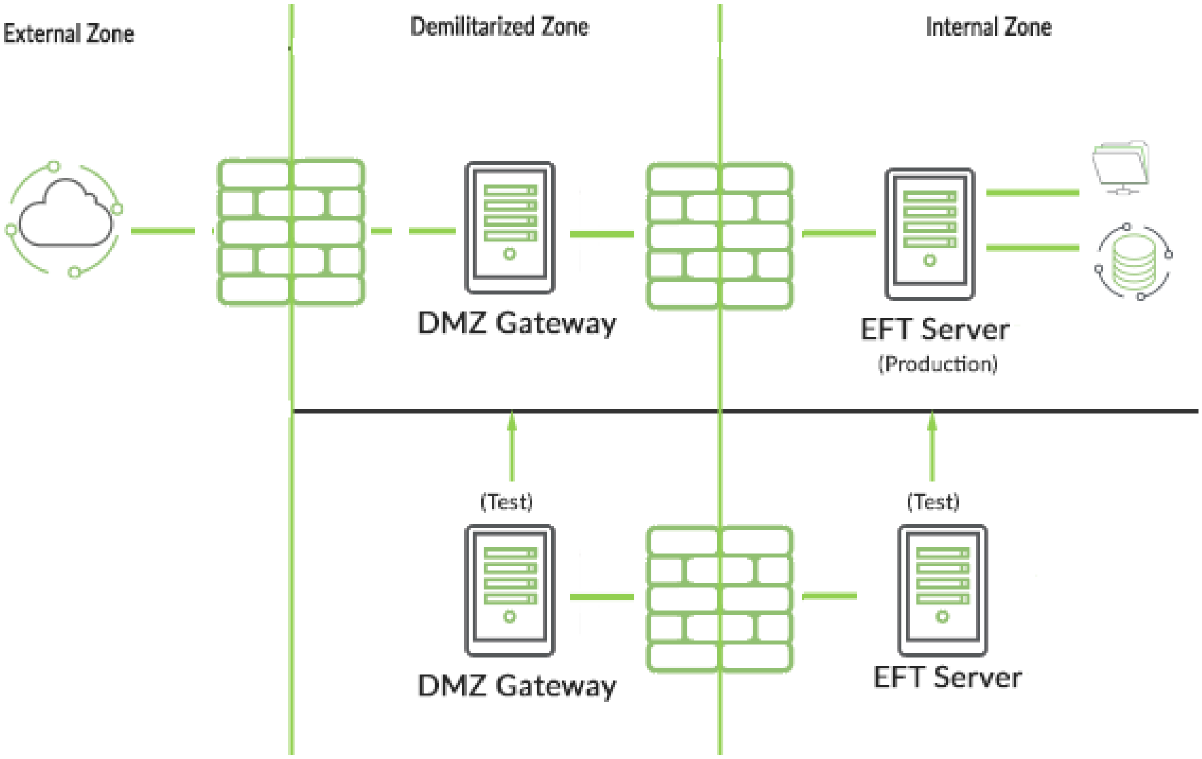


Figure 3 Development & Test environment

High Availability Environments (Clustering)

A group of tightly coupled computers that work together closely so that they can be viewed as though they are a single computer is a "cluster." A failover cluster has redundant nodes that are used to provide service when redundant system components fail.

EFT High Availability (HA) solution can protect your critical business processes and ensure that crucial file transfer systems are always on, and that employees, customers, and business partners experience seamless availability of critical applications and information.

EFT with HA can:

- Maintain availability through any planned or unplanned outage
- Increase stability and flexibility by implementing multiple nodes of EFT for load balancing
- Enhance throughput and better meet important SLAs by deploying multiple nodes of EFT to allow the collective environment to use more available resources
- Improve scalability with the ability to share common configurations across nodes, eliminating the challenge of having multiple servers set up with different configurations

In a clustered environment, two or more EFT servers within a cluster can access the same product database and user files at the same time. Clustering allows these systems to share security settings, user accounts, configurations, audit logs, and other product tables. If one EFT node fails, the remaining nodes in the cluster will automatically continue to process workloads and file transfer requests.

What's the difference between active-active and active-passive load balancing?

- An active-active cluster is typically made up of at least two nodes, both actively running the same kind of service simultaneously. The main purpose of an active- active cluster is to achieve load balancing. Load balancing distributes workloads across all nodes to prevent any single node from getting overloaded. Because there are more nodes available to serve, there will also be a marked improvement in throughput and response times.
- Like the active-active configuration, active-passive also consists of at least two nodes. However, as the name "active passive" implies, not all nodes are going to be active. In the case of two nodes, for example, if the first node is already active, the second node must be passive or on standby. The passive (a.k.a. failover) server serves as a backup that's ready to take over as soon as the active (a.k.a. primary) server gets disconnected or is unable to serve.

The clustering configurations described below include Active-Passive, Active-Active, and Active-Active for Disaster Recovery.

EFT Active-Passive Cluster

EFT Active-Passive Cluster is a high availability solution that provides fast automatic failover in case of application failure or node failure.

Requisitesfor EFT Cluster Mode, Active-Passive (Does not apply to Microsoft clustering)

- Load Balancer (if using DMZ Gateway)
- MSMQ Multicast or Unicast (configuration coherence, heartbeat, event rules coordination)
- Highly Available File Storage (NAS) (same datacenter)
- Database Server (Optional)
- EFT is configured for Active/Passive using failover in Event Rules
- 1 EFT Production license
- 1 EFT Non-Production license
- 1 DMZ Production license
- 1 DMZ Non-Production license

Benefits

- Highly Available End points (Inbound/outbound) and automation
- No downtime for OS patching and rebooting
- Automatic failover

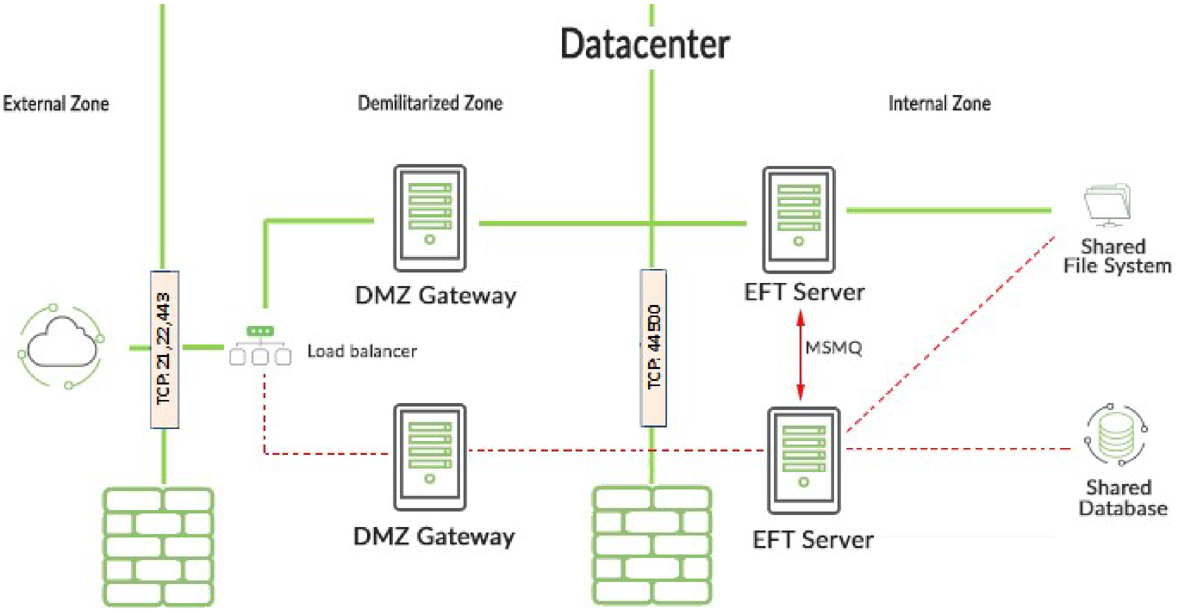


Figure 4 EFT Active-Passive Cluster

EFT Active-Active Cluster

EFT's active-active deployments provide HA using multiple instances of EFT and a load balancer for non-stop availability of your network. And unlike active-passive failover clusters, all the nodes in EFT's active-active deployment are put to work in production—with no standby hardware, and no clustering software. In this architecture, EFT is clustered with 2 or more servers for high availability, and the systems are installed in the private network. Associated DMZ Gateways are installed in the DMZ and no inbound ports are opened to the private network. The product and user files share configuration across each system/node in the cluster. A load balancer provides load balancing for incoming connections to DMZ Gateway, and the clustered EFT servers distribute the project workloads evenly across each node in the cluster.

Requisites for EFT Cluster Mode, Active-Active (Does not apply to Microsoft clustering)

- Load Balancer (if using DMZ Gateway)
- MSMQ Multicast or Unicast (configuration coherence, heartbeat, event rules coordination)
- Highly Available File Storage (NAS) (same datacenter)
- Database Server (Optional)
- 2 EFT Production licenses
- 2 DMZ Gateway Production licenses (if using DMZ Gateway)

Benefits

- Highly Available End points (Inbound/outbound) and automation
- Scale out with load balancing traffic and automation processing
- Scale out up to 16 nodes (usually in the same datacenter)
- Zero Downtime for any cluster maintenance. No downtime for OS patching and rebooting

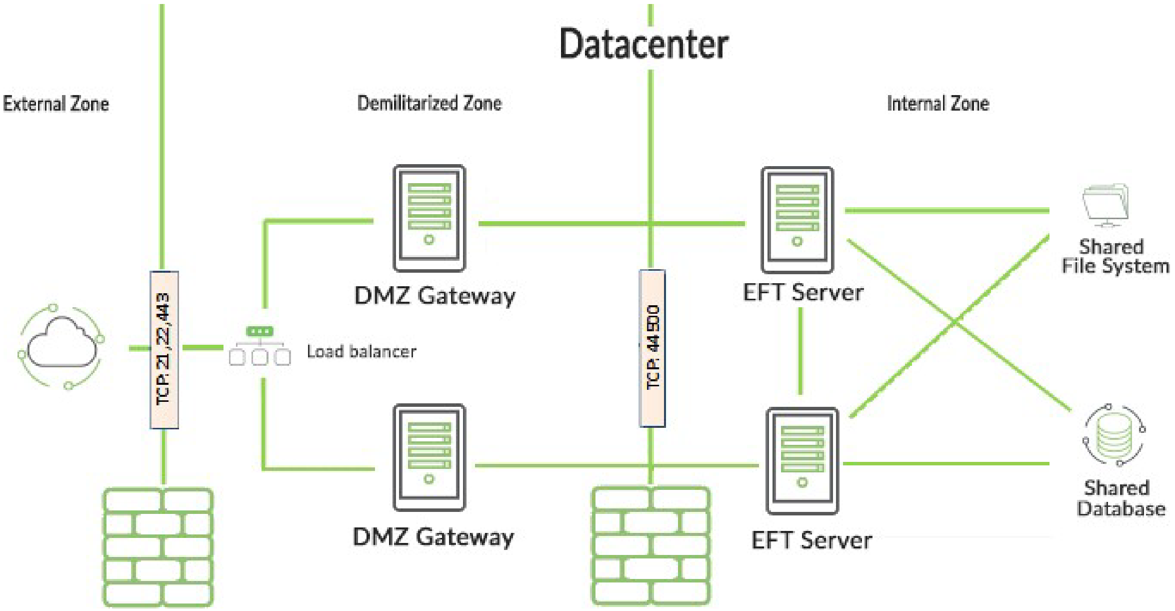


Figure 5 EFT Active-Active cluster

EFT Active-Active Cluster HA + Disaster Recovery

EFT's active-active deployments provide HA using multiple instances of EFT and a load balancer for non-stop availability of your network. And unlike active-passive failover clusters, all the nodes in EFT's active-active deployment are put to work in production—with no standby hardware, and no clustering software. In this architecture, EFT is clustered with 2 or more servers for high availability, and the systems are installed in the private network.

Associated DMZ Gateways are installed in the DMZ and no inbound ports are opened to the private network. The product and user files share configuration across each system/node in the cluster. A load balancer provides load balancing for incoming connections, and the clustered EFT servers distribute the project workloads evenly across each node in the cluster.

Benefits

- Highly Available Endpoints (Inbound/outbound) and automation
- Scale out with load balancing traffic and automation processing
- Disaster Recovery
- Scale-up to 16 nodes on each data center
- No downtime for OS patching and rebooting

EFT Active-Active Cluster HA + DR (Regular)

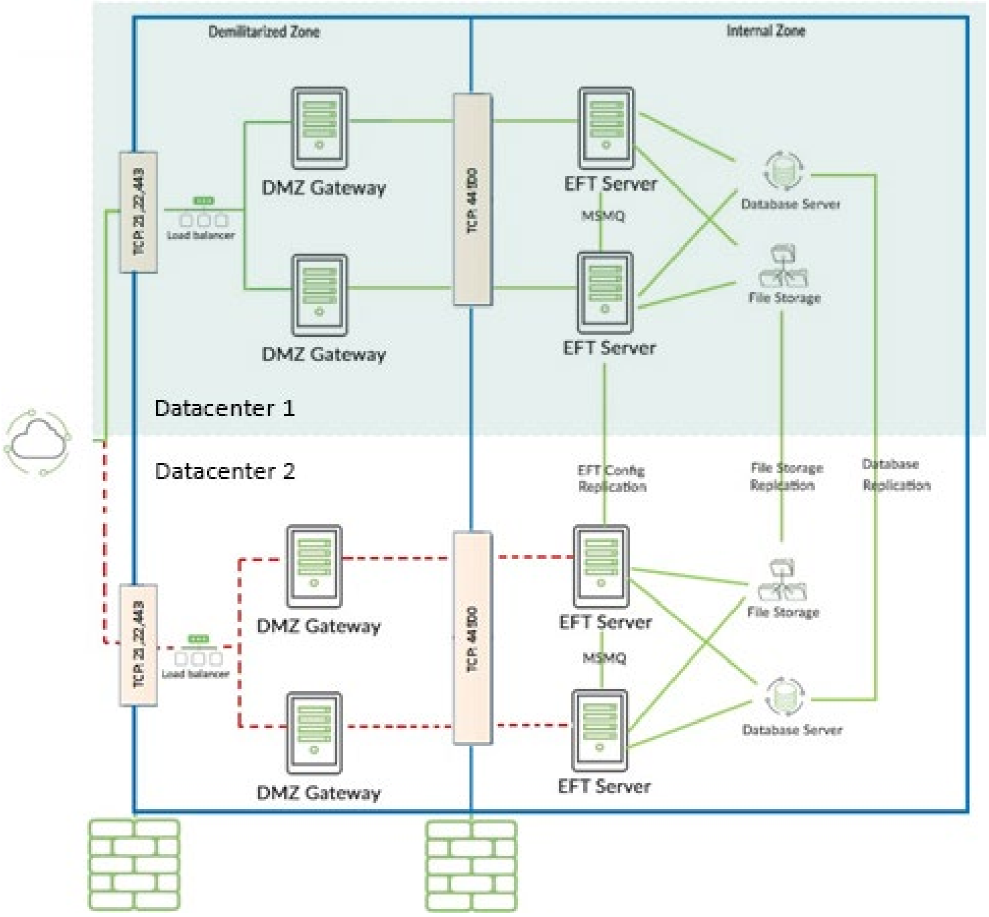


Figure 6 EFT Active-Active Cluster Disaster Recovery Regular

Requisites for EFT Cluster HA Mode, Active-Active + DR Regular

(Does not apply to Microsoft clustering)

- Global Load Balancer or DNS manager for failover
- Load Balancer
- MSMQ Multicast or Unicast (configuration coherence, heartbeat, event rules coordination) between all nodes in both data centers
- Highly Available File Storage (NAS) across data centers, share file locks among all nodes of each cluster for EFT HA Share Config and EFT Share Data
- Database HA Server Cluster across data centers
- 2 EFT and 2 DMZ Production licenses
- 2 EFT and 2 DMZ Standby licenses

EFT Active-Active Cluster HA Mode + DR (Mission Critical)

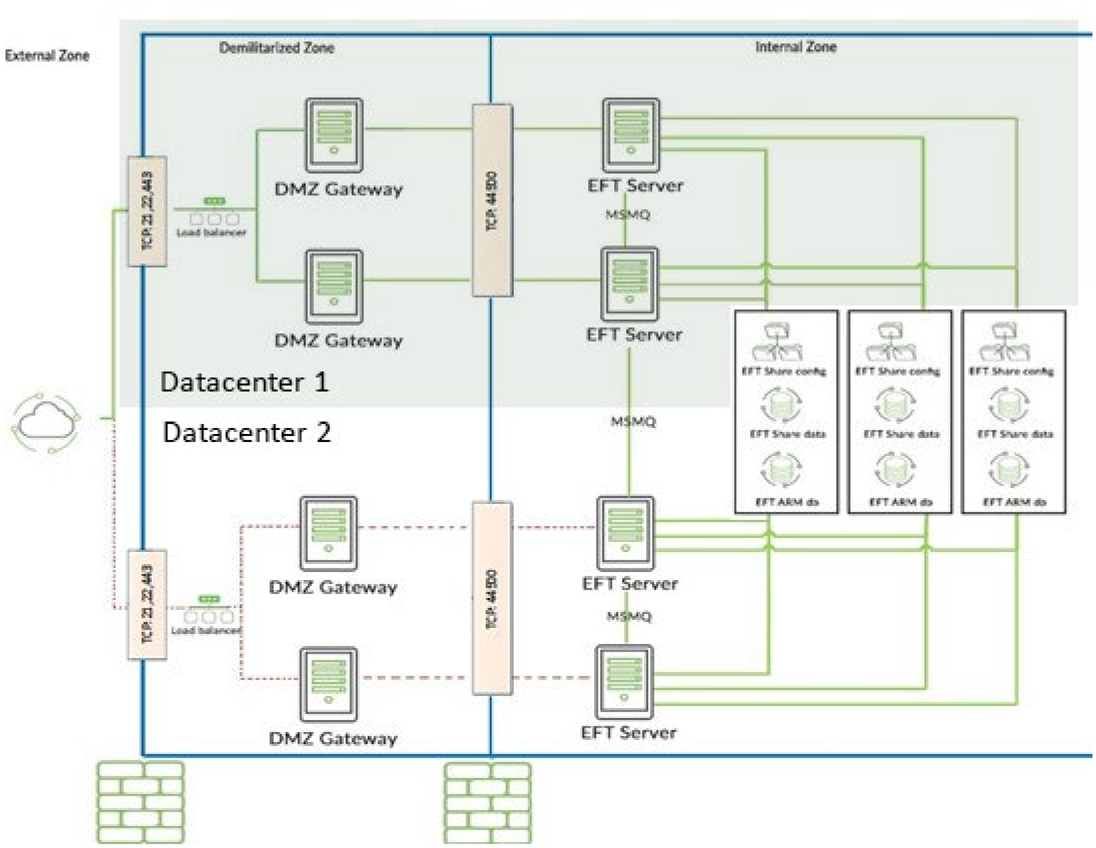


Figure 7 EFT Active-Active Cluster Disaster Recovery Mission Critical

Requisites for EFT Cluster HA Mode, Active-Active + DR Mission Critical

(Does not apply to Microsoft clustering):

- Global Load Balancer or DNS manager for failover
- Load Balancer
- MSMQ Multicast or Unicast (configuration coherence, heartbeat, event rules coordination) within each data center
- Highly Available File Storage (NAS) with replication or synchronization between data centers, share file locks among all nodes of each cluster
- Database Server (Optional) with database replication technologies
- 2 EFT and 2 DMZ Production licenses
- 2 EFT and 2 DMZ Non-Production licenses

EFT in the Cloud

With a self-managed cloud deployment of Globalscape EFT, companies can enjoy the benefits of the cloud, including scalability, flexibility, and affordability, while reducing the size of their own data centers. By minimizing their software costs, number of data servers, and other related resources, organizations can significantly decrease IT expenses without reducing IT capabilities.

Deploy EFT through Microsoft Azure or Amazon Web Services (AWS) and in minutes you can securely transfer data to and from the cloud. Buy an EFT license and install it on your own instance in Azure or AWS, designed however you need it. You install, manage, and control your data.

Businesses that use the cloud benefit from high utilization and smooth transactions, ready to handle operational workload peaks and valleys. These companies also see improvements with operational efficiency, reduced overhead costs, enhanced agility, and rapid deployment readiness.

Additionally, if you already have an on-premises installation of EFT and the Cloud Connector Module, you can configure automated cloud storage monitoring for AWS S3 and Azure Blobs, and support for automation processes such as uploading or downloading files to/from Amazon S3 or Azure Blob storage.

Globalscape's "Bring Your Own License" (BYOL) model lets you pay once to purchase a license that includes all EFT features. You can deploy that license on-premises, in a private cloud, or any public cloud of your choice. Globalscape also offers a subscription license which would ensure that your EFT installation is always the most up-to- date version with the latest security updates.

A Cloud MFT deployment supplements your EFT Sites with:

- Easy trial experience
- Extensive global footprint with multiple regions around the world
- Strong service-level agreements
- Automate data exchanges between people and systems
- Gain visibility into the movement of files
- Replace legacy, or homegrown file sharing systems
- Securely share files internally or externally
- Enable compliance with corporate, industry, and government mandates
- Ensure uptime of your mission-critical infrastructure
- Additional cloud-service tools and services such as load balancing, storage redundancy, replication to a second region, site recovery, automatic OS image upgrade, security patching, and others.

For assistance in installing and configuring your self-managed EFT installation in the cloud, refer to the following articles or ask your account manager about Professional Services.

- EFT Running on Azure in the Cloud
- Enable Azure AD SSO with EFT Arcus and the Web Transfer Client
- Amazon EC2 Instance Deployment Guide for Standalone EFT Enterprise POC AWS EFT Usage Instructions

The two cloud services are described in Microsoft Azure and Amazon AWS below.

Microsoft Azure

Globalscape EFT is certified compatible with Microsoft Azure. In Azure, you can configure a virtual machine (VM) with the latest Windows operating system, then install and configure EFT (as a single server) and any EFT modules that you have licensed. After EFT is installed and configured, you can connect to it as you would any other EFT installation. During the Azure setup, you configure the DNS location to which users and other servers can connect, such as myeftserveronazure.com.

Availability zones expand the level of control you must maintain the availability of the applications and data on your VMs. An Availability Zone is a physically separate zone, within an Azure region. There are three Availability Zones per supported Azure region. Each Availability Zone has a distinct power source, network, and cooling. By designing your solutions to use replicated VMs in zones, you can protect your apps and data from the loss of a data center. If one zone is compromised, then replicated apps and data are instantly available in another zone.

Microsoft recommends that two or more VMs are created within an availability set to provide a highly available application and to meet the 99.95% Azure SLA. Combine the Azure Load Balancer with an availability zone or availability set to get the most application resiliency. The Azure Load Balancer distributes traffic between multiple virtual machines.

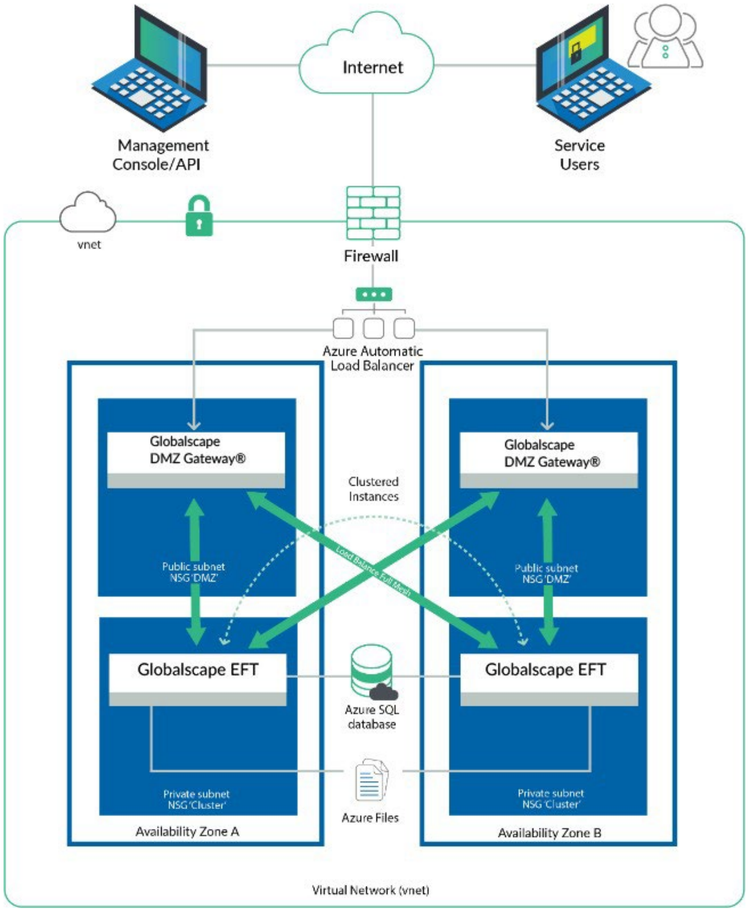


Figure 8 EFT in Microsoft Azure

Microsoft Azure Performance Recommendations

The following table provides storage and database recommendations for small -to medium-size deployments and enterprise-level deployments.

Minimum deployments are defined as having:

- Under 25k daily inbound and outbound transactions
- Files sizes under 250 MB
- Under 5k daily workflow jobs comprised of SQL, data translation, Web Service calls, and PGP

Recommended deployments are defined as having:

- Under 50k daily inbound and outbound transactions
- Files sizes under 500 MB
- Under 10k daily workflow jobs comprised of SQL, data translation, Web Service calls, and PGP

High Performance deployments are defined as having:

- Over 50k daily inbound and outbound transactions
- Over 10k daily workflow jobs comprised of SQL, data translation, Web Service calls, and PGP

Deployment Size	Application Server Size	Storage	Database
Minimum	One general purpose virtual machine (Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dpdsv5, Dpldsv5, Dpsv5, Dplsv5, Dv4, Dsv4, Ddv4, Ddsv4, Dv5, Dsv5, Ddv5, Ddsv5, Dasv5, Dadsv5) with 2 Cores & 4 GB RAM	Azure Files: General purpose version 2 (GPv2) storage accounts	Azure SQL Database (vCore Purchasing Model): General Purpose
Recommended	Two general purpose virtual machines (Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dpdsv5, Dpldsv5, Dpsv5, Dplsv5, Dv4, Dsv4, Ddv4, Ddsv4, Dv5, Dsv5, Ddv5, Ddsv5, Dasv5, Dadsv5) with 4 Cores & 8 GB RAM	Azure Files: Premium File Shares	Azure SQL Database (vCore Purchasing Model): General Purpose
High Performance	Two or more general purpose virtual machines (Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dpdsv5, Dpldsv5, Dpsv5, Dplsv5, Dv4, Dsv4, Ddv4, Ddsv4, Dv5, Dsv5, Ddv5, Ddsv5, Dasv5, Dadsv5) with 8 Cores & 16 GB RAM	Azure Files: Premium File Shares	Azure SQL Database (vCore Purchasing Model): Business- critical or Hyperscale

Amazon AWS

Leverage the Amazon AWS infrastructure to power your managed file transfer system, Globalscape EFT. With Globalscape EFT deployed in AWS, IT teams can use the industry- leading services and tools available in AWS.

With a self-managed deployment model, you can leverage your own resources to manage your infrastructure. The EFT BYOL license can be installed on an Amazon Machine Image (AMI) in the Amazon Marketplace. With this deployment model you can decide which AWS instance size to run the AWS AMI based on the demands of your business. EFT will provide intra- and inter-region high availability when deployed across multiple Availability Zones (AZ), providing more protection against failures in case of a single zone outage.

- Multiple DMZ Gateway systems provide high availability for the reverse proxy.
- EFT is protected by the DMZ Gateway proxy servers in the DMZ. No inbound ports need to be opened into the private cloud network. No files are stored in the private cloud.
- All incoming connections are distributed across each system in the cluster.
- Advanced Workflow Projects and Jobs are distributed across multiple systems.
- If one EFT Site experiences a failure, another system in the cluster will automatically take over.
- Leverages the performance improvements of a cloud system, database, and file storage solution.

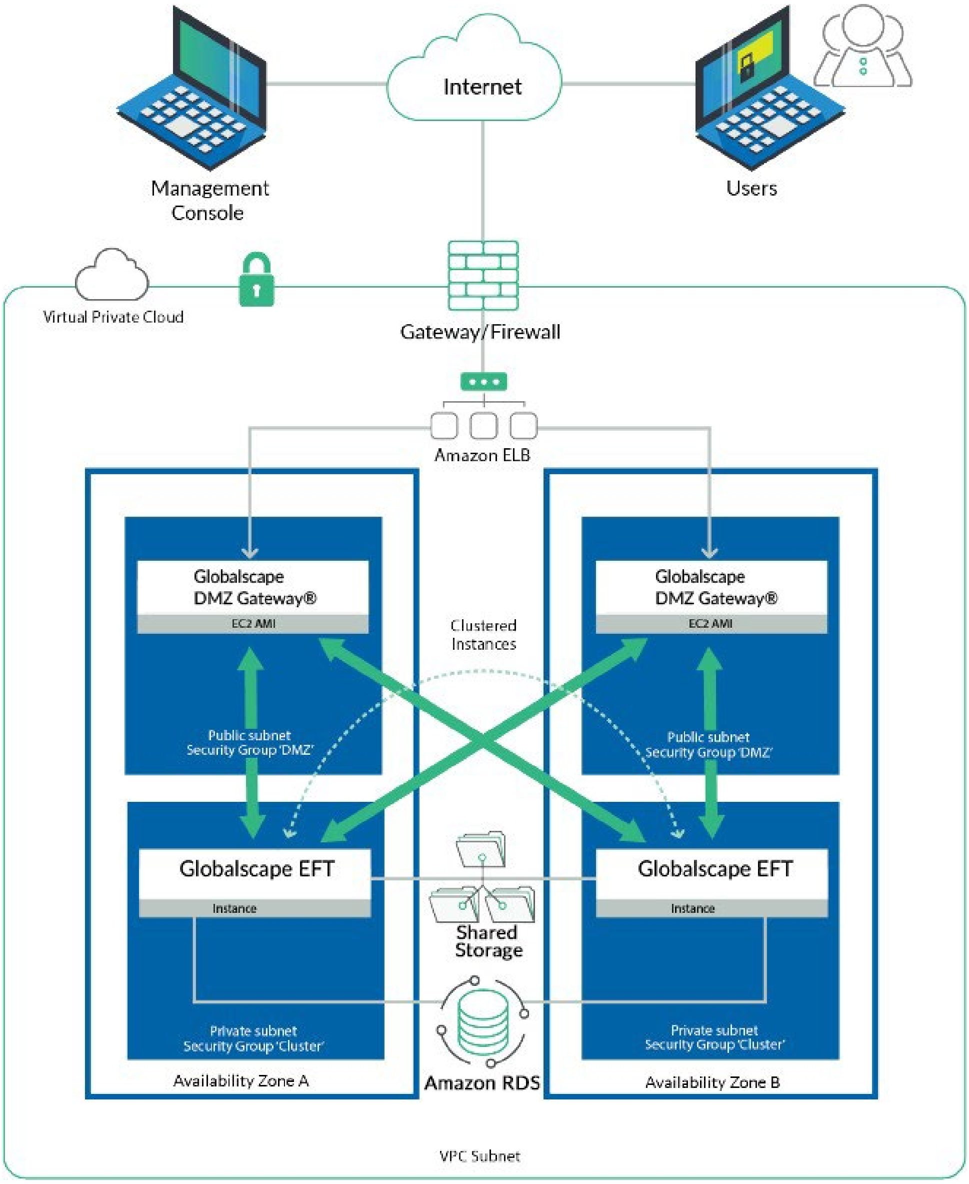


Figure 9 EFT in Amazon AWS

Amazon AWS EC2 Performance Recommendations

The following table provides storage and database recommendations for small- to medium- size deployments and enterprise-level deployments.

Minimum deployments are defined as having:

- Under 25k daily inbound and outbound transactions
- Files sizes under 250 MB
- Under 5k daily workflow jobs comprised of SQL, data translation, Web Service calls, and PGP

Recommended deployments are defined as having:

- Under 50k daily inbound and outbound transactions
- Files sizes under 500 MB
- Under 10k daily workflow jobs comprised of SQL, data translation, Web Service calls, and PGP

High Performance deployments are defined as having:

- Over 50k daily inbound and outbound transactions
- Over 10k daily workflow jobs comprised of SQL, data translation, Web Service calls, and PGP

NOTE: Load testing in UAT or staged environments for definitive environment settings that suit your organization's requirements is recommended.

Clustered EFT with Two Sites on Amazon EC2

Deployment Size	Application Server Size	Storage	Database
Minimum	One medium EC2 T3 Instances	EFS File System General purpose performance mode Bursting throughput mode	RDS Production template Provisioned IOPS at 2000
Recommended	Two LargeEC2 T3 instances	Shared Storage, File Share (SMB or CIFS) access via UNC path required. Latency from EFT to share <25MS	RDS Production template Provisioned IOPS at 40000
High Performance	Two or more XlargeEC2 T3 instances	Shared Storage, File Share (SMB or CIFS) access via UNC path required. Latency from EFT to share <25MS	RDS Production template Provisioned IOPS at 60000

AWS Storage Options

EFT HA requires a file share for user's files and shared configuration. EFT access these file shares using SMB 3 protocol and reference them with an UNC path. Below are some storage options that can be used with EFT as a share.

- **Windows File Shares** using EC2 instances.
- **Amazon FSx** for Windows File Server.
- **AWS Storage Gateway** with Amazon FSx for Windows File Server or Amazon S3
  - To avoid EFT HA issues, you must disable the use of opportunistic locking. Make sure you deselect the **Activate** option for **Opportunistic lock (oplock) when you create the SMB file share**. Create an SMB file share with custom configuration.

Amazon RDS Options

Amazon RDS for SQL Server is fully managed by Amazon Relational Database Service (RDS). The following options can be used for EFT:

- ***Amazon RDS for SQL Server***.
  - *Production*: Use Production template. It's recommended to use SQL Server Standard or Enterprise edition as engines. GP2, GP3, IO1 storage type and allocated storage minimum of 60GB. Multi-AZ (Mirroring/Aways On) should be use for HA deployments for availability and durability.
  - *Dev/Test*: Use Dev/Test template. You could also use SQL Server Express Edition as engine. GP2, GP3, IO1 storage type and allocated storage minimum of 20GB.
- ***Amazon RDS for Oracle***.
  - *Production*: Use Production template. It's recommended to use Oracle Enterprise Edition or Standard Edition. GP2, GP3, IO1 storage type and allocated storage minimum of 60GB. Multi-AZ (Mirroring/Aways On) should be used for HA deployments for availability and durability.
  - *Dev/Test*: Use Dev/Test template. You could also use Oracle Standard Edition Two as the engine. GP2, GP3, IO1 storage type and allocated storage minimum of 20GB.

ICAP Threat Protection & DLP Considerations

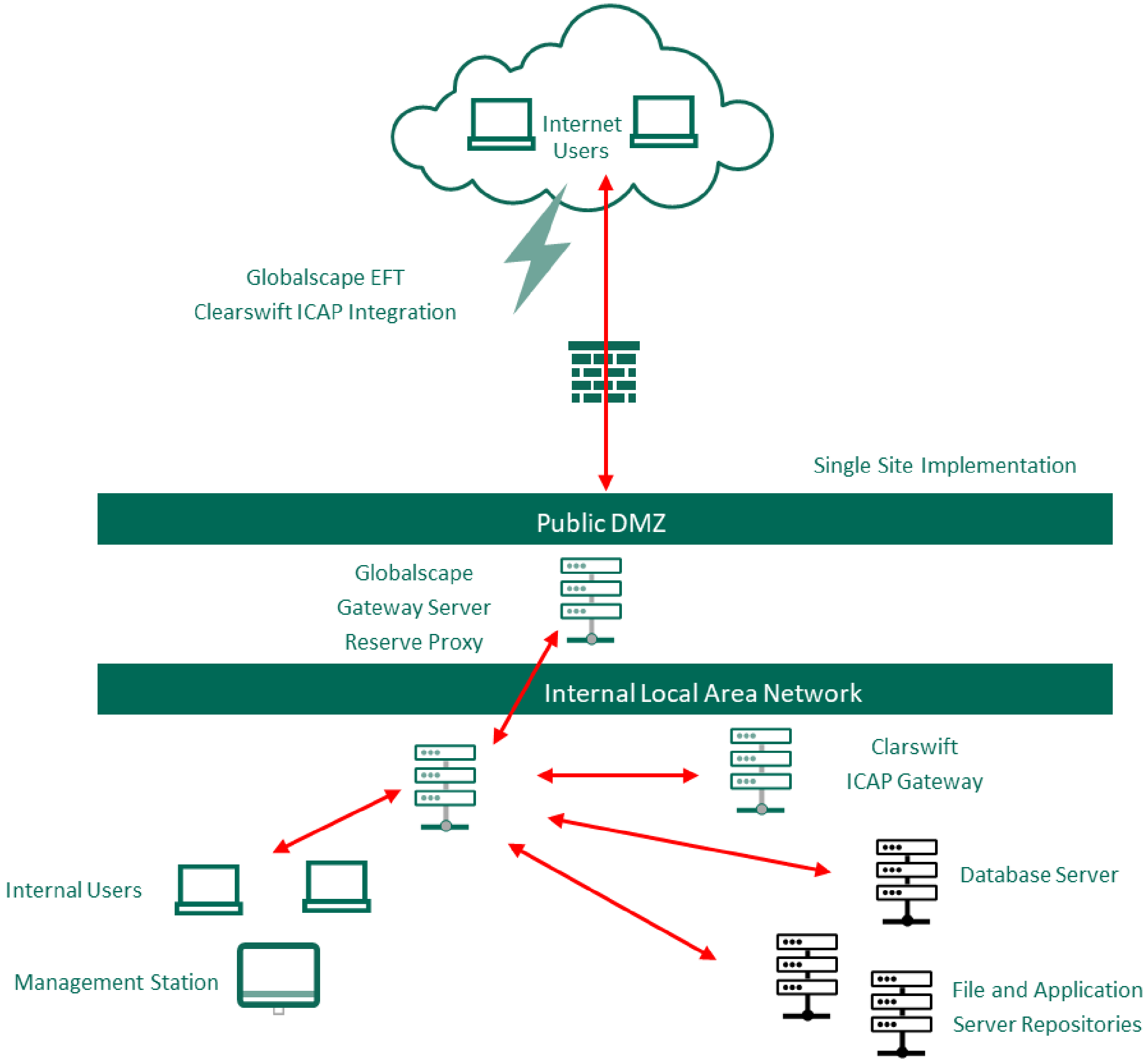
As part of an all-encompassing data security strategy, organizations need to secure and protect content that is uploaded or downloaded from the web or shared via MFT solutions.

The Clearswift Secure ICAP Gateway complements existing web proxy infrastructures and MFT software to provide an added layer of data security. A deep content inspection engine detects sensitive or critical data, active and malicious threats and then applies the appropriate remedial action, allowing safe content to flow through, reducing business disruption.

- The Clearswift Secure ICAP Gateway enhances the ability for EFT to control information by applying deep content inspection and Adaptive Data Loss Prevention.
- EFT uses the Clearswift Secure ICAP Gateway to inspect, detect, and clean metadata and revision history in files being transferred.
- EFT is protected by the DMZ Gateway proxy servers in the DMZ. No inbound ports need to be opened into the private cloud network. No files are stored in the private cloud.
- Data loss is mitigated since the product database and user files are stored on a separate server than the EFT Site.
- Leverages the performance improvements of an enterprise database system and file storage solution.
- Content scanning controls can be placed on inbound or outbound files.

Single DMZ Gateway, Single EFT, and a Single Clearswift ICAP Gateway

In this architecture, a single DMZ Gateway in the DMZ on an internal network/LAN is installed with a single EFT server and a single Clearswift ICAP Gateway positioned near the EFT server.



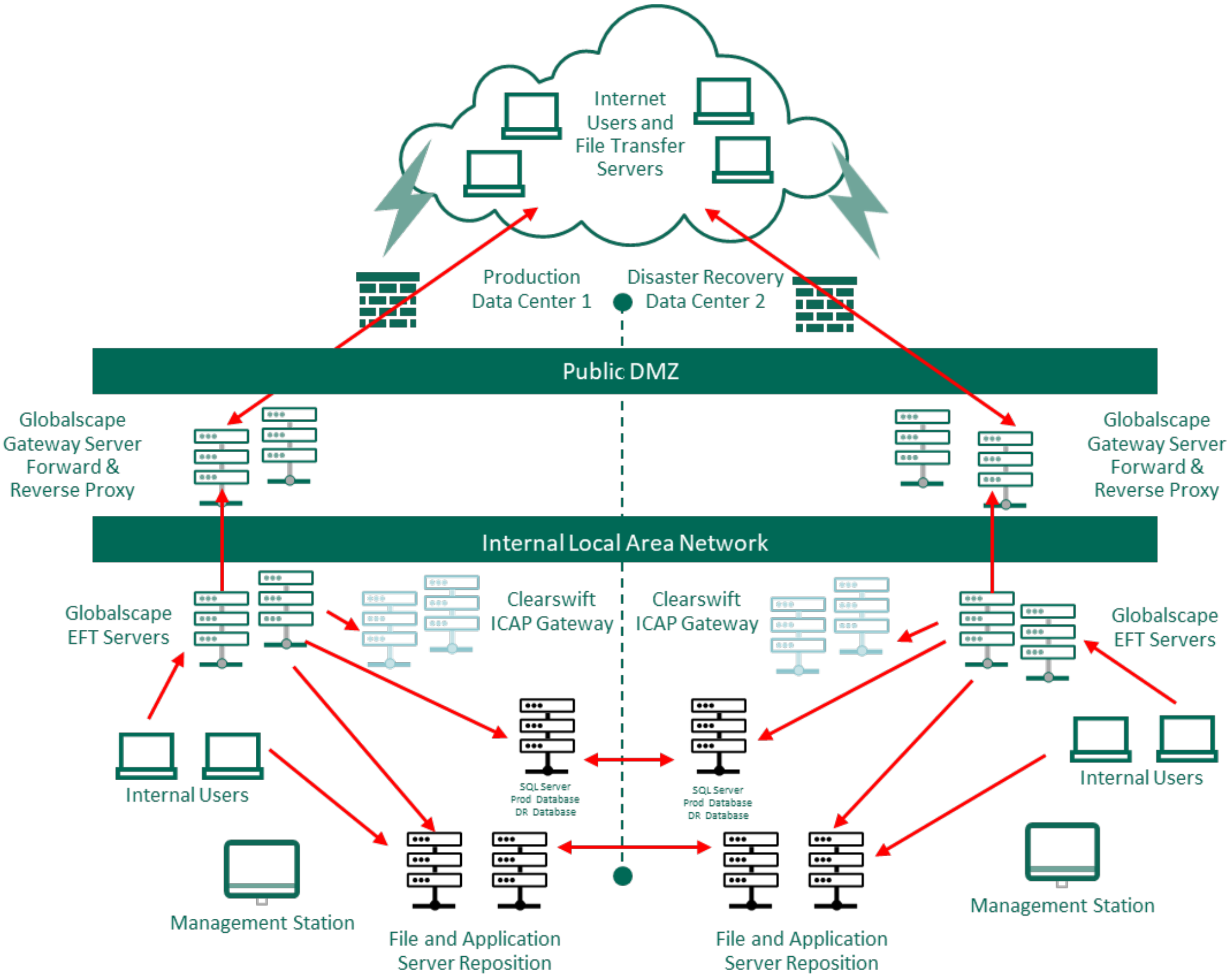
Clustered DMZ Gateway and MFT Clustered Clearswift ICAP Gateways

In this architecture, multiple DMZ Gateways are positioned in a DMZ on an internal network/LAN along with multiple EFT servers installed within an internal network. Multiple Clearswift ICAP Gateways are also installed within the same internal network.

In this architecture, the number of Clearswift ICAP Gateways is can be architected by:

- One Clearswift ICAP Gateway per EFT server
- Multiple Clearswift ICAP Gateways per EFT server
- One Clearswift ICAP Gateway per site

Considerations such as number of files, size of files content scanning rules, and period that file scan should complete within can all be factored into the decision-making process. Fortra has also performed load simulations which can be provided upon request.



Internet Users and File Transfer Servers
Production Data Center 1
Disaster Recovery Data Center 2
Public DMZ
Globalscape Gateway Server Forward & Reverse Proxy
Globalscape Gateway Server Forward & Reverse Proxy
Internal Local Area Network
Globalscape EFT Servers
Clearswift ICAP Gateway
Clearswift ICAP Gateway
Globalscape EFT Servers
SQL Server Prod Database DR Database
SQL Server Prod Database DR Database
Internal Users
Internal Users
Management Station
Management Station
File and Application Server Reposition
File and Application Server Reposition

Zero Trust File Transfer Bundle

Most file transfer solutions have been designed to transfer sensitive information when using secure connections and encryption to protect data. However, secure connections as well as encryption algorithms such as PGP may be inadequate if there is not 100% trust and data is sensitive. A few examples are:

- Files are sent via email. After download/decryption, unencrypted file is forwarded to unauthorized recipient
- Files land via SFTP on shared storage. After decryption, file and/or contents can easily be shared

Fortra's Digital Rights Management solution can secure any type of file in cloud or on-premises when used in conjunction with EFT. Security policies follow the file which allows IT security teams to define granular usage rights that control how files are used and distributed, even once they are stored on devices outside of your network.

You can then track any file and use granular controls to prevent unauthorized access and revoke privileges at any time. If data ever leaks or is downloaded from EFT, Fortra's Digital Rights Management security sticks to the file anywhere it goes, making sure that only authorized parties are working with your company's information.

Please contact your EFT Account Manager to learn more about this solution. You can also review more information about the Zero Trust File Transfer Bundle.

- Authenticate each access point, verify every identity, and limit access.
- Encrypt data end-to-end, allowing access via secure email download links.
- Provide visibility and real-time analytics to monitor and detect threats.
- Instantly revoke access to shared files and services.
- For encrypted files and documents, rotate PGP keys frequently for maximum security.

Incorporate Alert Logic Web Access Firewall (WAF)

Web applications are important to your business and a vital part of how customers interact with you. Unfortunately, they also give attackers another gateway into your critical assets and data. Businesses need to accurately distinguish good traffic from bad traffic in real-time.

Fortra Managed Web Application Firewall (WAF) provides you with a highly versatile, fully managed, enterprise-level, and cloud-ready solution supported by our team of experts.

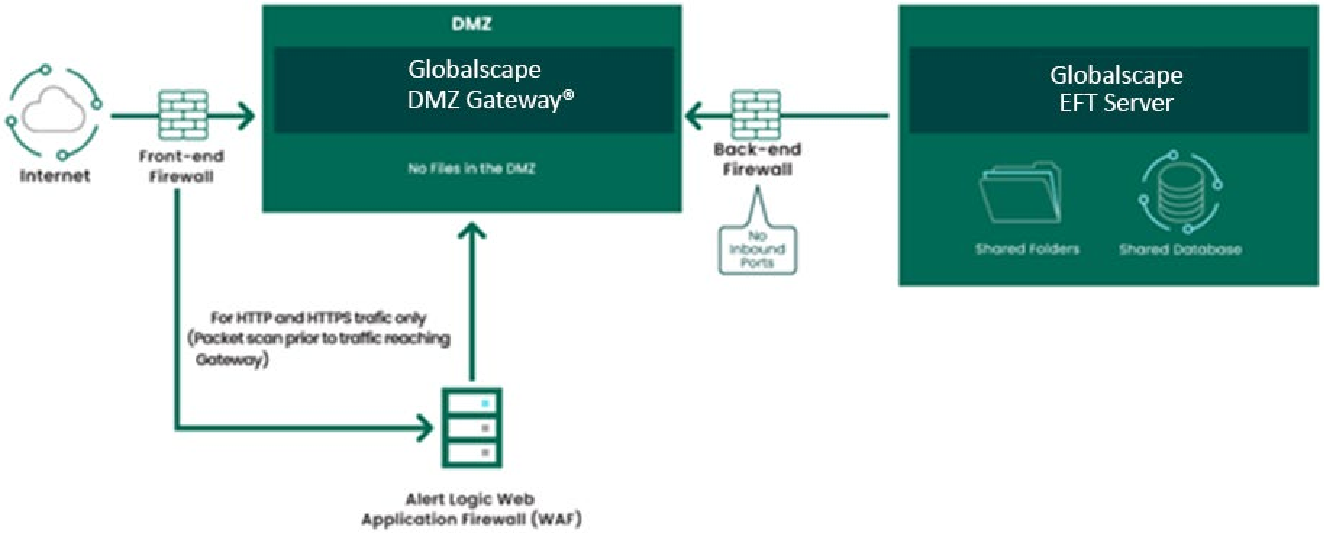
Please contact your Account Manager to learn more about this solution. You can also review the Web Application Firewall datasheet.

- Fortra's Managed WAF service includes installation and deployment services to ongoing configuration, ensuring your WAF is ready to block threats against your critical web applications.
- Out-of-the-box policies cover more than10,000 vulnerabilities, including unique flaws in off-the-shelf and custom web applications (e.g., OWASP Top 10, URL tampering, web scraping, buffer overflow attacks, zero-day web application threats, credential stuffing attacks, API attacks, and DoS attacks).
- Our analysts fine-tune your WAF by monitoring your web application traffic, whitelisting valid requests and data, and building a policy that blocks malicious web traffic and other undesired activities. Our experts become an extension of your security team, eliminating the complexity of policy building and challenges of ongoing threat management.
- Built-in Fortra Threat Intelligence is used to track the evolution of tactics and techniques in the web security space, as well as maintaining a repository of active malicious actor IP addresses and attack campaigns including emerging threats.
- Additional security layer for your MFT environment.

Architecture

The Alert Logic Web Application Firewall (WAF) can be implemented:

- With a single DMZ Gateway and EFT Site
- With multiple DMZ Gateways and EFT Sites
- On-premises or within your AWS or Azure cloud infrastructure



Internet
Front-end Firewall
DMZ
Globalscape DMZ Gateway®
No Files in the DMZ
Back-end Firewall
No Inbound Ports
Globalscape EFT Server
Shared Folders
Shared Database
For HTTP and HTTPS trafic only (Packet scan prior to traffic reaching Gateway)
Alert Logic Web Application Firewall (WAF)