GoAnywhere MFT System Architecture Guide

Copyright Terms and Conditions

Table of Contents

INTRODUCTION

Overview

GoAnywhere MFT is a managed file transfer (MFT) solution which streamlines the exchange of data between your systems, employees, customers, and trading partners. It provides a single point of control with extensive security settings, detailed audit trails, and reports.

GoAnywhere MFT's intuitive interface and comprehensive workflow features can help eliminate the need for custom programs/scripts, single-function tools, and manual processes that were traditionally needed. This innovative solution can reduce costs, improve the quality of your file transfers, and help your organization comply with data security policies and regulations.

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

GoAnywhere MFT can be scaled horizontally by adding additional systems to the cluster.

When paired with a load balancer like GoAnywhere Gateway™, inbound connections to the file servers can be distributed to the available systems in the cluster. For file transfers performed in Advanced Workflows (Projects), clustering allows the workload to be distributed across all systems to increase performance and throughput. As your business and transfer requirements grow, GoAnywhere MFT can easily grow with it by adding additional systems to the cluster.

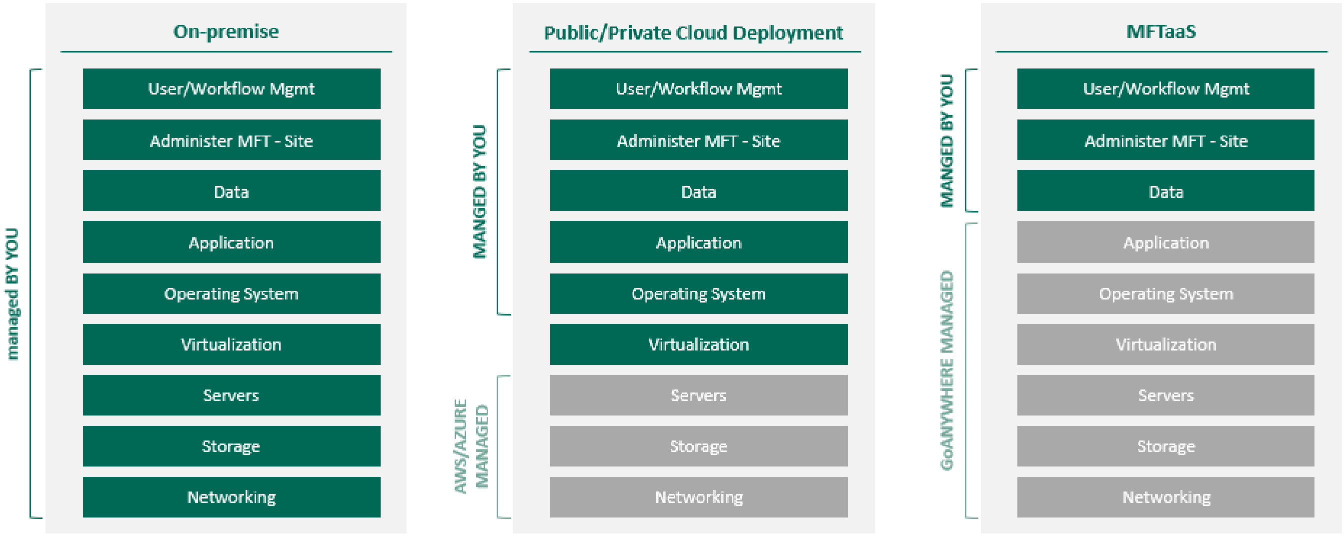
This guide describes several common GoAnywhere MFT architectures, demonstrating support for high availability (clustering) and load balancing, as well as the advantages of each configuration.

Ensuring data backup, disaster recovery, and high availability for your GoAnywhere MFT system focuses on three key areas:

- **GoAnywhere MFT Software and License** – The program files required for GoAnywhere MFT to run
- **Product Database** – Stores the configuration settings and application data used to run GoAnywhere MFT
- **User Files** – The folders for storing user documents and miscellaneous GoAnywhere settings

Which Deployment is Right for me?

GoAnywhere is Operating System agnostic and supports On-Premises or Cloud deployments. GoAnywhere also provides a SaaS platform.



On-premise

managed BY YOU

- User/Workflow Mgmt
- Administer MFT - Site
- Data
- Application
- Operating System
- Virtualization
- Servers
- Storage
- Networking

Public/Private Cloud Deployment

MANGED BY YOU

- User/Workflow Mgmt
- Administer MFT - Site
- Data
- Application
- Operating System
- Virtualization

AWS/AZURE MANAGED

- Servers
- Storage
- Networking

MFTaaS

MANGED BY YOU

- User/Workflow Mgmt
- Administer MFT - Site
- Data

GoANYWHERE MANAGED

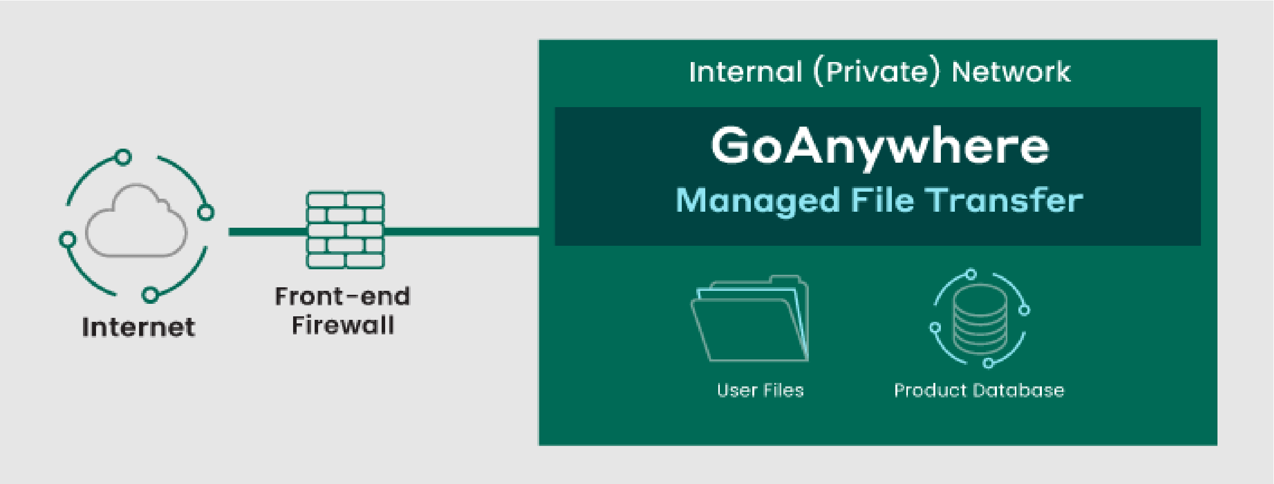
- Application
- Operating System
- Virtualization
- Servers
- Storage
- Networking

SINGLE MFT SYSTEM

Default

In this architecture, GoAnywhere MFT is installed behind the corporate front-end firewall. If file transfer services are enabled, ports to the HTTP/S, FTP, FTPS, SFTP, AS2, and AS4 protocols are opened on the firewall to allow all inbound connections to GoAnywhere.

The default stand-alone system uses the embedded Derby database, and the user files are located within the GoAnywhere MFT installation directory.



Comments

- Ideal for small operations where a moderate number of files are being transferred and redundancy, high availability, and disaster recovery are not required.

EXTERNAL DATABASE AND USER FILES

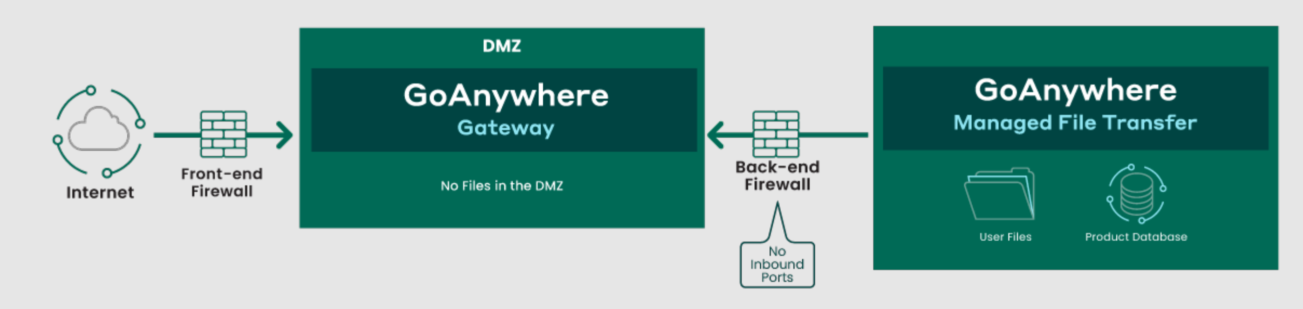
In this architecture, the product database has been externalized to use a database vendor of your choice. The user files have been configured to use an external file server.

Comments

- Data loss is mitigated since the product database and user files are stored on a separate server than the GoAnywhere MFT system.
- Leverages the performance improvements of an enterprise database system and file storage solution.

External Gateway

In this architecture, GoAnywhere MFT is installed in the Private Network and GoAnywhere Gateway is installed in the demilitarized zone (DMZ). No inbound ports are opened into the Private Network, and no files are stored in the DMZ.



Comments

- GoAnywhere MFT is protected by the GoAnywhere Gateway proxy server in the DMZ. No inbound ports need to be opened into the private network. No files need to be stored in the DMZ.
- GoAnywhere Gateway acts as an Enhanced Reverse Proxy and Forward Proxy for GoAnywhere MFT. This allows your internet connections to remain in the DMZ while keeping your sensitive data inside your firewall when external users upload or download data from GoAnywhere MFT.
- GoAnywhere Gateway also acts as a load balancer and can scale with your MFT needs.

HIGH AVAILABILITY ENVIRONMENTS

Overview

In this architecture, multiple GoAnywhere MFT systems are installed behind the corporate front-end firewall. If file transfer services are enabled, ports to the HTTP/S, FTP, FTPS, SFTP, AS2, and AS4 protocols are opened on the firewall to allow all inbound connections to GoAnywhere.

Clustering

Clustering allows two or more GoAnywhere MFT systems to work together to allow workloads to be distributed horizontally across multiple GoAnywhere MFT installations. In a clustered environment, two or more GoAnywhere MFT systems within a cluster can connect to the same product database and user files simultaneously.

This allows these systems to share security settings, trading partner user accounts, configurations, audit logs, and other product tables. If one GoAnywhere MFT system fails, the remaining systems in the cluster will automatically continue to process workloads and file transfer requests.

This active-active clustered environment also provides the best high-availability option for handling potential system failures. If one GoAnywhere MFT system fails, the remaining systems in the cluster will automatically continue to service the trading partners.

GOANYWHERE GATEWAY

GoAnywhere Gateway is both an enhanced reverse proxy and forward proxy. It provides an additional layer of network security when your organization needs to safely exchange data with your trading partners. When using GoAnywhere Gateway as a reverse proxy, no inbound ports need to be opened into the private/internal network and no sensitive data needs to be stored in the DMZ.

GoAnywhere Gateway is a software-only solution which is installed in the DMZ or public-facing network. Trading partners only connect to authorized GoAnywhere MFT ports, on which routes requests over a proprietary channel to back-end services (for example, FTP, SFTP, HTTPS), in the private/internal network. This approach allows your organization to keep sensitive information (for example, data files, user credentials, keys, certificates) in the private/internal network, keeping your DMZ in compliance.

When GoAnywhere Gateway is used as a forward proxy for outbound connections, it will hide the identities and locations of those internal systems.

In essence, GoAnywhere Gateway serves as a transparent interface between internal systems and external systems without exposing sensitive files and the private/internal network. This is an essential solution for meeting strict security policies and complying with state privacy laws, HIPAA, PCI DSS, SOX, ISO 27000, and GLBA.

Load Balancing

GoAnywhere Gateway can serve as a load balancer for distributing connections across multiple GoAnywhere MFT systems within a cluster. This active-active framework provides greater high availability for mission-critical environments.

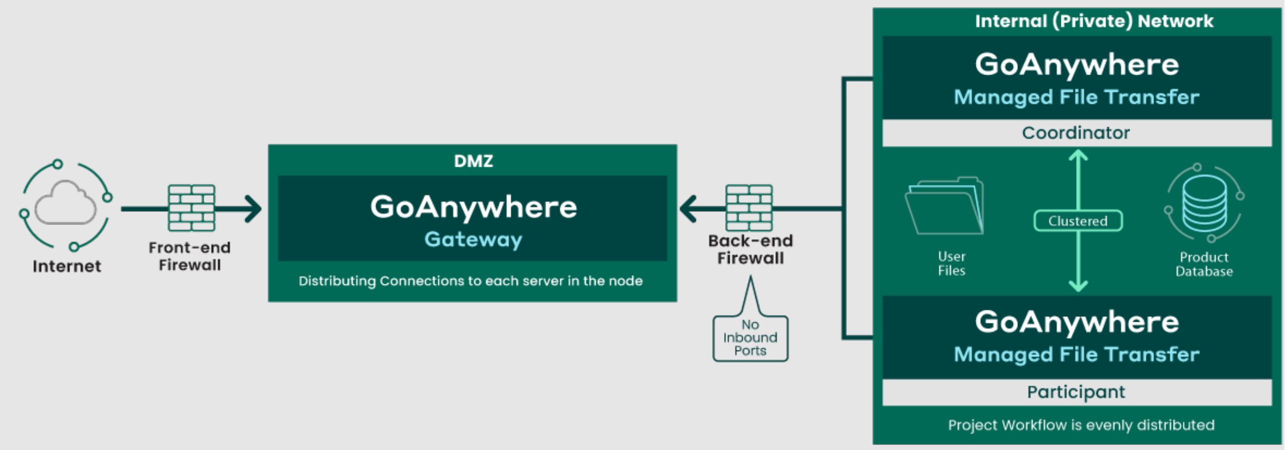
As a load balancer, GoAnywhere Gateway spreads connections evenly across the clustered systems. This load-balancing algorithm is called “round-robin,” which is a common load-balancing standard.

CLUSTERED MFT SYSTEMS

With Single Gateway

In this architecture, GoAnywhere MFT is clustered with two or more systems for high availability, and the systems are installed in the Private Network. GoAnywhere Gateway is installed in the DMZ and no inbound ports are opened to the Private Network.

The product database and user files have been externalized to share across each system in the cluster. GoAnywhere Gateway is providing load balancing for incoming connections, and the clustered GoAnywhere MFT systems are distributing the project workloads evenly across each system in the cluster.



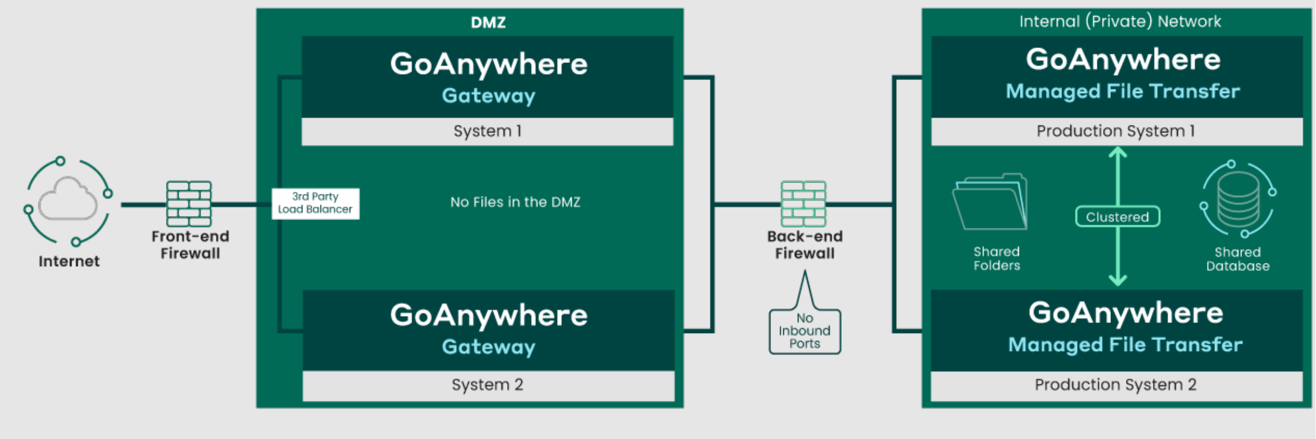
Comments

- GoAnywhere MFT is protected by the GoAnywhere Gateway proxy server in the DMZ. No inbound ports need to be opened into the private network. No files need to be stored in the DMZ.
- All incoming connections are equally distributed across each system in the cluster.
- Workflow Jobs are distributed across multiple systems.
- If one GoAnywhere MFT system experiences a failure, another system in the cluster will automatically take over.
- Leverages the performance improvements of an enterprise database system and file storage solution.
- Additional Gateways as well as MFT servers can be added if needed.

With Two Gateways

In this architecture, GoAnywhere MFT is clustered with two or more systems for high availability, and the systems are installed in the Private Network. A third-party load balancer is distributing inbound connections across two GoAnywhere Gateways, which are installed in the DMZ, and no inbound ports are opened to the Private Network.

The product database and user files have been externalized to share across each system in the cluster. Each GoAnywhere MFT system in the cluster is configured to use each Gateway, and the clustered GoAnywhere MFT systems are distributing the project workloads across each system in the cluster.



Comments

- Multiple GoAnywhere Gateway systems are providing high availability for the reverse proxy.
- GoAnywhere MFT is protected by the GoAnywhere Gateway proxy servers in the DMZ. No inbound ports need to be opened into the private network. No files need to be stored in the DMZ.
- All incoming connections are distributed across each system in the cluster.
- Advanced Workflow Projects and Jobs are distributed across multiple systems.
- If one GoAnywhere MFT system experiences a failure, another system in the cluster will automatically take over.
- Leverages the performance improvements of an enterprise database system and file storage solution.
- Additional Gateways as well as MFT servers can be added if needed.

DISASTER RECOVERY

Basic Considerations

While clustering ensures the GoAnywhere MFT system will continue running if a single system has failed, disaster recovery (DR) ensures you have an adequate backup and recovery solution in a situation where your entire production site fails.

There are several ways to incorporate Disaster Recovery into a GoAnywhere architecture. A few examples are below:

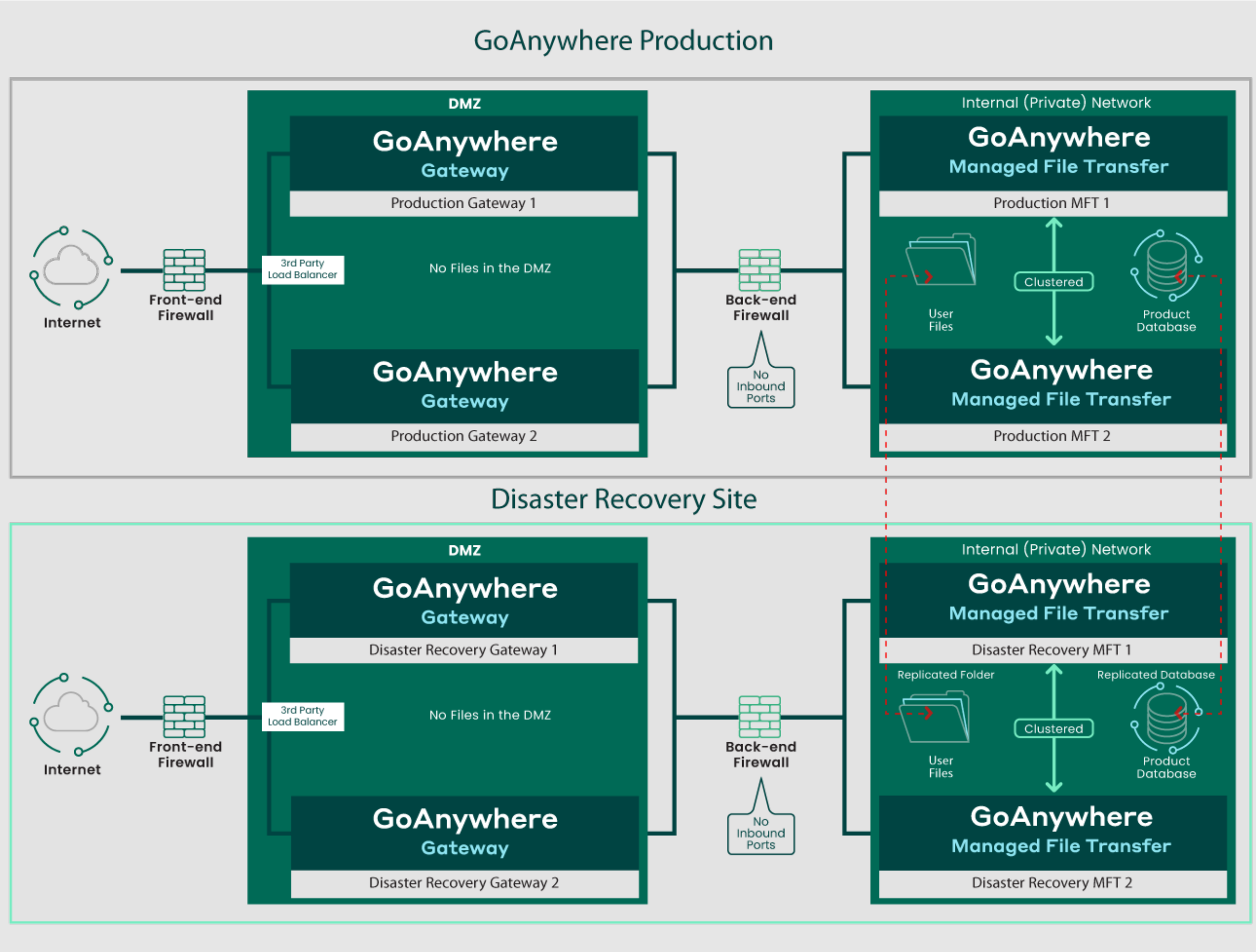
- Single GoAnywhere Gateway *plus* single GoAnywhere MFT server in Production as well as DR
- Multiple GoAnywhere Gateways *plus* multiple GoAnywhere MFT servers *in* Production as well as DR
- Multiple GoAnywhere Gateways *plus* multiple GoAnywhere MFT servers *in* Production
- Single GoAnywhere *plus* multiple GoAnywhere MFT servers *and* DR
- Single GoAnywhere Gateway *plus* multiple GoAnywhere MFT servers *in* Production
- Single GoAnywhere Gateway *plus* single GoAnywhere MFT server *in* DR

In the disaster recovery example below, the production GoAnywhere MFT is clustered with two or more systems for high availability, and the systems are installed in the Private Network.

A third-party load balancer is sending inbound connections across two GoAnywhere Gateways, which are installed in the DMZ, and no inbound ports are opened to the Private Network. The product database and user files have been externalized to share data across each system in the production cluster and for replication to the disaster recovery site.

The disaster recovery site also contains redundant Gateways and clustered GoAnywhere MFT systems. If the production system becomes unavailable, the DR site can come online with the replicated user files and replicated product database.

NOTE: *It is your responsibility to replicate the user files and product database using a third-party solution.*



DISASTER RECOVERY USING AN ONLINE LICENSE

Online licenses include a ‘Restricted Disaster Recovery’ feature. This allows the replication of an instance for a brief period of time. When an online license that was activated on one system is used on another system, GoAnywhere will enter Limited Mode. While in Limited mode, users will be unable to add Web Users, Resources, or Projects.

If the primary system goes down, and it becomes necessary for the replicated instance to become the primary, the license will remain valid as long as it is only being used for one system.

Deactivating a current license will deactivate the primary and secondary system. The license page in GoAnywhere MFT allows an admin to activate a new license without deactivating the current license. See the GoAnywhere MFT Users Guide within our customer portal for more information.

DISASTER RECOVERY USING A STANDARD LICENSE

If you have not purchased the disaster recovery feature with your standard license but would like to test the process, you can request a temporary license ahead of time. Once the system is replicated or restored from the backup or DR instance, simply remove the .lic file, restart GoAnywhere, and activate the temporary license. You will then be able to test the DR instance on the temporary evaluation license.

If your primary instance is down and you need to use the DR instance long-term, deactivate the paid license and then reactivate it. This will reset the MAC address assigned to the license. For more information, see the GoAnywhere MFT User Guide within our customer portal.

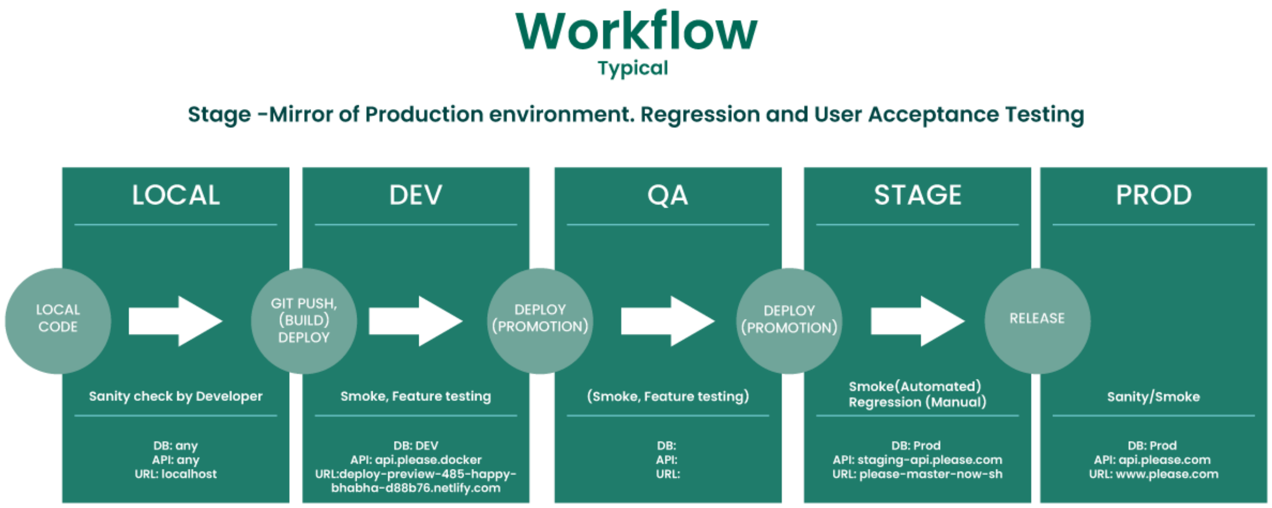
If a permanent Disaster Recovery license is required, it must be purchased and can be procured through your account manager.

UAT/QA/STAGING AND DEVELOPMENT

Fortra recommends that customers include additional GoAnywhere MFT licenses for development and/or testing purposes. Doing so will help when implementing best practices surrounding the development of new workflows, business use cases, quality assurance, and security best practices without impacting Production.

- Extra licenses are helpful for providing change control and quality assurance of new workflows that you build in GoAnywhere MFT
- This architecture facilitates testing of new releases/patches provided by Fortra in an isolated environment, Minimizing Production downtime
- UAT and Development environments are ideal for performing routine load testing, helping you scale Production resources to meet forecasted growth demands
- This architecture allows you to install and test the latest version of GoAnywhere before updating Production, mitigating incompatibility issues

GoAnywhere MFT includes tools to allow authorized users to promote workflows, schedules, and other items from a Development/Test environment into Production.



CLOUD COMPUTING

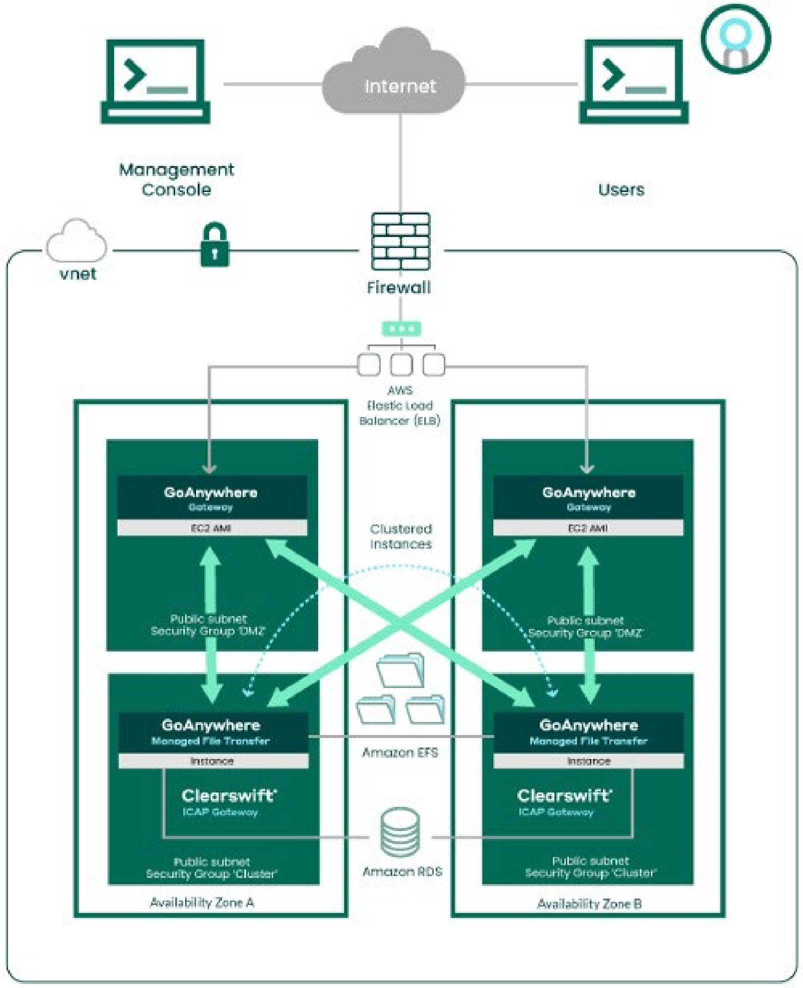
Amazon (AWS)

Clustered MFT with Two Gateways on Amazon EC2

In this architecture, GoAnywhere MFT is installed on two Amazon Machine Images (AMI).

GoAnywhere is clustered for high availability, and the systems are installed in Amazon's Private Cloud Network. GoAnywhere Gateway is installed in the DMZ within each Availability Zone, and no inbound ports are opened to the Private Cloud Network.

The product database and user files have been externalized to Amazon's Relational Database Service (RDS) and Amazon's Elastic File System (EFS) to share data across each system in the cluster. Each GoAnywhere MFT system in the cluster is configured to use each Gateway, and the clustered GoAnywhere MFT systems are distributing the project workloads evenly across each system in the cluster.


Internet
Management Console
Users
vnet
Firewall
AWS Elastic Load Balancer (ELB)
GoAnywhere Gateway
EC2 AMI
Public subnet Security Group 'DMZ'
Clustered Instances
GoAnywhere Gateway
EC2 AMI
Public subnet Security Group 'DMZ'
GoAnywhere Managed File Transfer
Instance
Clearswift ICAP Gateway
Public subnet Security Group 'Cluster'
Availability Zone A
Amazon EFS
Amazon RDS
GoAnywhere Managed File Transfer
Instance
Clearswift ICAP Gateway
Public subnet Security Group 'Cluster'
Availability Zone B

Comments

- Multiple GoAnywhere Gateway systems provide high availability for the reverse proxy.
- GoAnywhere MFT is protected by the GoAnywhere Gateway proxy servers. No inbound ports need to be opened into the Virtual Private Cloud (VPC). No files are stored outside the VPC.
- All incoming connections are distributed across each system in the cluster.
- Advanced Workflow Projects and Jobs are distributed across multiple systems.
- If one GoAnywhere MFT system 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.

Amazon AWS EC2 Performance Recommendations

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

Small- to medium-size deployments are defined as having:

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

Enterprise-level 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: *Fortra recommends load testing in UAT or **staged environments** for definitive environment settings that suit your organization's requirements.*

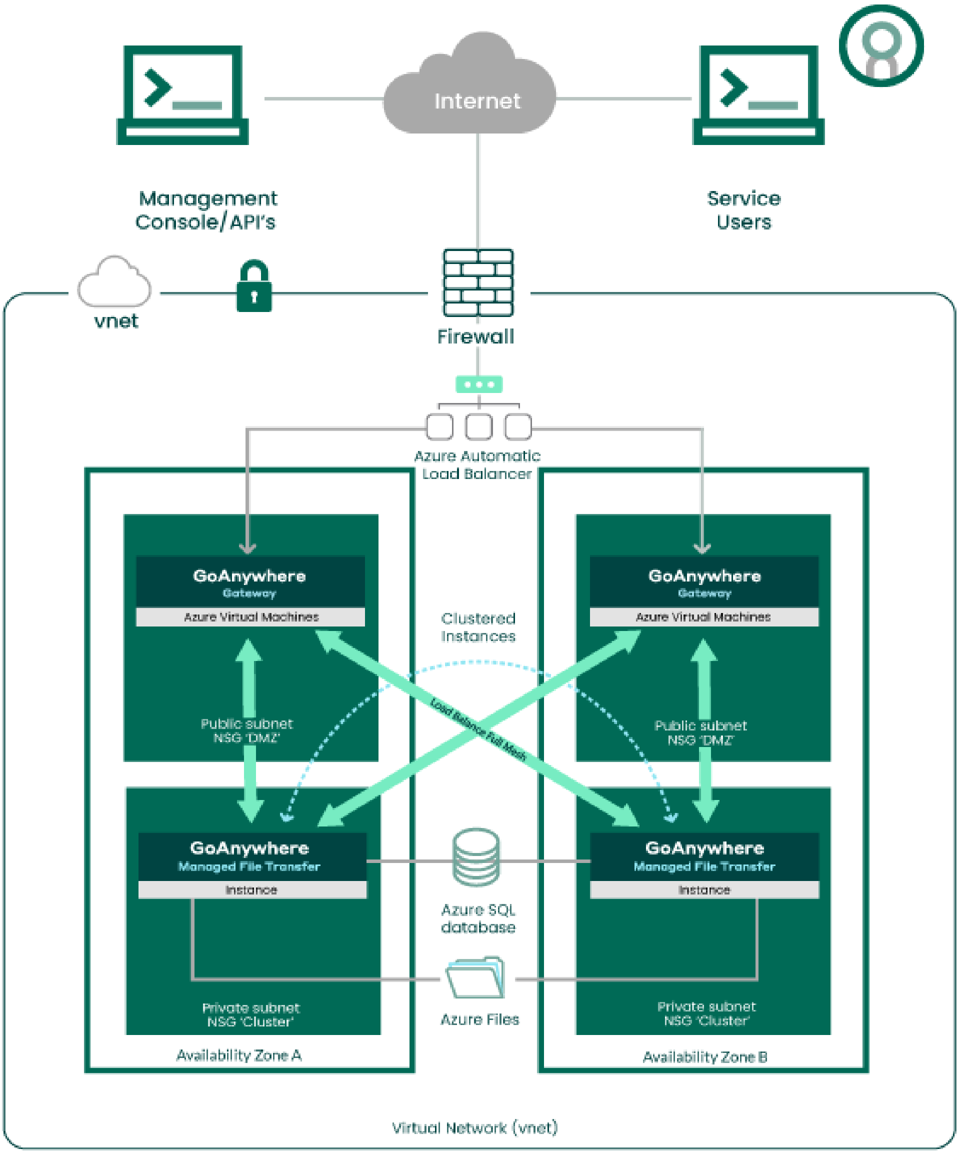
Clustered MFT with Two Gateways on Amazon EC2

Deployment Size	Application Server Size	Storage	Database
Small to medium	Two medium EC2 T3 instances	EFS File System General purpose performance mode Bursting throughput mode	RDS Production template Provisioned IOPS at 40000
Enterprise	Two or more large EC2 T3 instances	EFS File System Max IO performance mode Bursting throughput mode	RDS Production template Provisioned IOPS at 60000

MICROSOFT AZURE

Clustered MFT with Two Gateways on Azure

In this architecture, GoAnywhere MFT is clustered for high availability, and the systems are installed in Azure's Private Cloud Network. GoAnywhere Gateway is installed in the DMZ within each Availability Zone, and no inbound ports are opened to the Private Cloud Network. The product database and user files have been externalized to Azure's SQL Database Service (RDS) to share data across each system in the cluster. Each GoAnywhere MFT system in the cluster is configured to use each Gateway, and the clustered GoAnywhere MFT systems are distributing the project workloads evenly across each system in the cluster.



Comments

- Multiple GoAnywhere Gateway systems provide high availability for the reverse proxy.
- GoAnywhere MFT is protected by the GoAnywhere 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 GoAnywhere MFT system 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.

Microsoft Azure Performance Recommendations

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

Small- to medium-size deployments are defined as having:

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

Enterprise-level 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
Small to medium	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 & 16 GB RAM	Azure Files: General purpose version 2 (GPv2) storage accounts	Azure SQL Database (vCore Purchasing Model): General Purpose
Enterprise	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 & 32 GB RAM	Azure Files: storage accounts	Azure SQL Database (vCore Purchasing Model): Business-critical or Hyperscale

FORTRA-FIED SECURITY ADD-ONS

ICAP Threat Protection & Data Loss Prevention (DLP) Considerations

Overview

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.

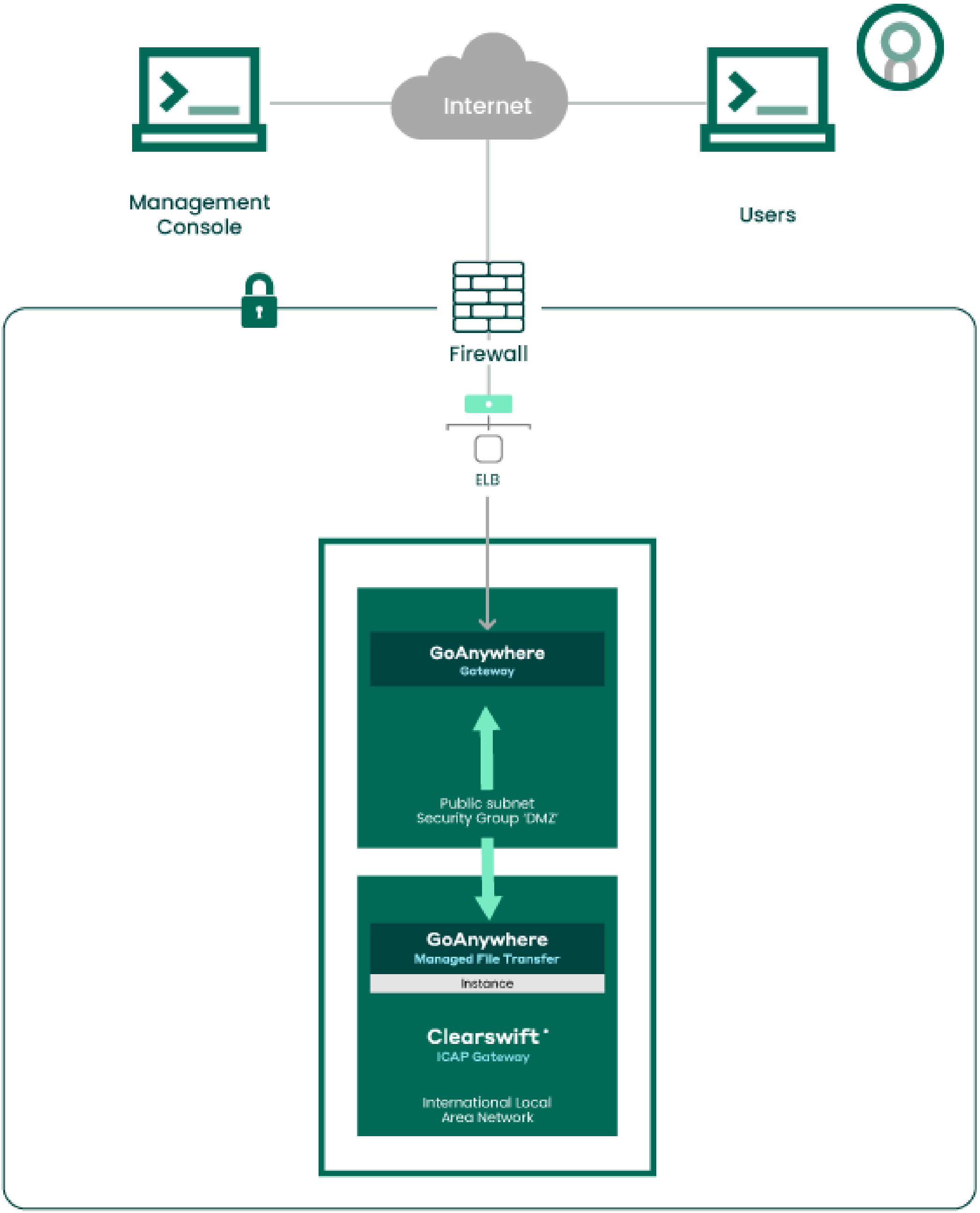
The Clearswift Secure ICAP Gateway complements existing web proxy infrastructures and MFT software to provide an added layer of data security. A deep content inspection engine detects sensitive or critical data, active and malicious threats, and then applies the appropriate remedial action, allowing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

Comments

- The Clearswift Secure ICAP Gateway enhances GoAnywhere's ability to control information by applying deep content inspection and Adaptive Data Loss Prevention.
- GoAnywhere uses the Clearswift Secure ICAP Gateway to inspect, detect, and clean metadata and revision history in files being transferred.
- GoAnywhere MFT is protected by the GoAnywhere 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 GoAnywhere MFT system.
- 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 GoAnywhere Gateway, single GoAnywhere MFT and a single Clearswift ICAP Gateway

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



Clustered GoAnywhere Gateway's & MFT Clustered Clearswift ICAP Gateways

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

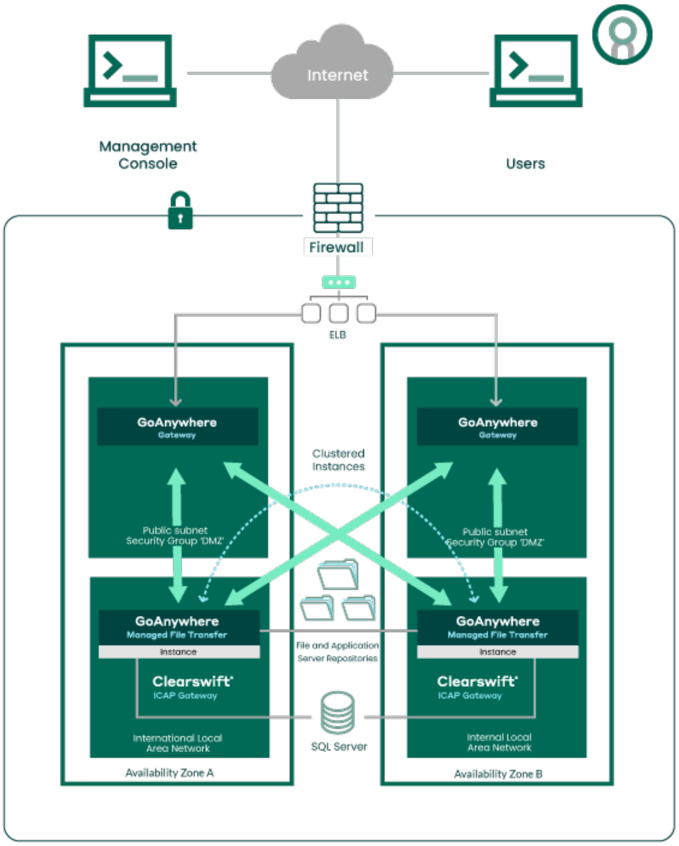
In this architecture, the number of Clearswift ICAP Gateways is can be architected by:

- One Clearswift ICAP Gateway per GoAnywhere MFT Server
- Multiple Clearswift ICAP Gateways per GoAnywhere MFT Server
- One Clearswift ICAP Gateway per site

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

GoAnywhere's workflows automate file transfers while the Secure ICAP Gateway identifies and neutralizes threats.

Please contact your GoAnywhere Account Manager to learn more about Clearswift Secure ICAP Gateway. You can review the Clearswift Secure ICAP Gateway datasheet (csw-secure-icap-gateway-ds.pdf (fortra.com)).


Internet
Management Console
Users
Firewall
ELB
GoAnywhere Gateway
Public subnet Security Group 'DMZ'
Clustered Instances
GoAnywhere Gateway
Public subnet Security Group 'DMZ'
GoAnywhere Managed File Transfer
Instance
Clearswift ICAP Gateway
International Local Area Network
File and Application Server Repositories
SQL Server
GoAnywhere Managed File Transfer
Instance
Clearswift ICAP Gateway
Internal Local Area Network
Availability Zone A
Availability Zone B

Zero Trust File Transfer Bundle

Overview

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 un-authorized recipient
- Files land on SFTP or shared storage. After decryption, file and/or contents can easily be shared

Fortra's Zero Trust File Transfer solution can secure any type of file in cloud or on-premises when used in conjunction with GoAnywhere. 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 GoAnywhere, Fortra's zero Trust File protection that adds access control and security that sticks to the file anywhere it travels.

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

Comments

- Never trust, always verify: 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)

Overview

Web applications (Including GoAnywhere) 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 approved traffic from malicious threat actors 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 GoAnywhere Account Manager to learn more about this solution. You can also review the Web Application Firewall datasheet.

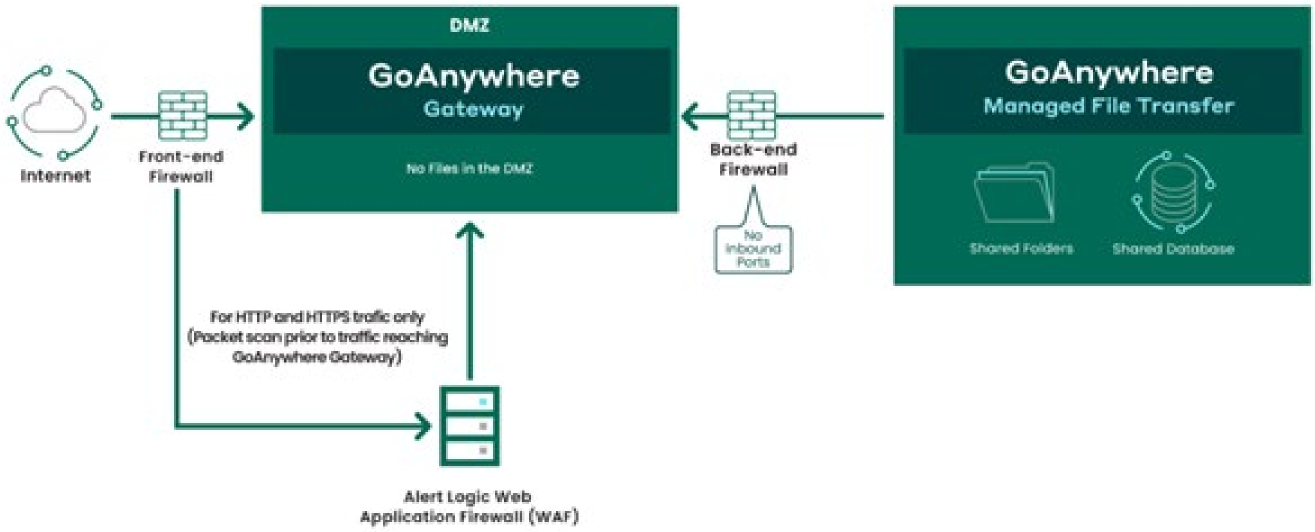
Comments

- 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 than 10,000 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 GoAnywhere Gateway and MFT server
- With multiple GoAnywhere Gateways and MFT servers
- On Premises or within your AWS or Azure cloud infrastructure



GOANYWHERE PERFORMANCE CONSIDERATIONS

Sizing Heavy Load Environments

GoAnywhere & Clearswift Stress Testing

Fortra's Clearswift pairs with GoAnywhere to provide complete and consistent protection across email, web, and endpoints to allow teams to collaborate securely and effectively while providing IT with needed control and visibility over sensitive data.

The Fortra GoAnywhere and Clearswift teams together have executed load testing against their platforms to provide benchmarks which can be used to properly architect our solutions. More information about content scanning using Clearswift is provided in the Add-Ons section.

The stress test guide is available upon request and outlines the performance of the following simulations:

- GoAnywhere MFT with GoAnywhere Gateway
- GoAnywhere MFT, GoAnywhere Gateway with Clearswift's Secure ICAP Gateway to scan all files for threats as well as banned media types.

The document also reviews system modifications to tweak system performance if this capability is required.