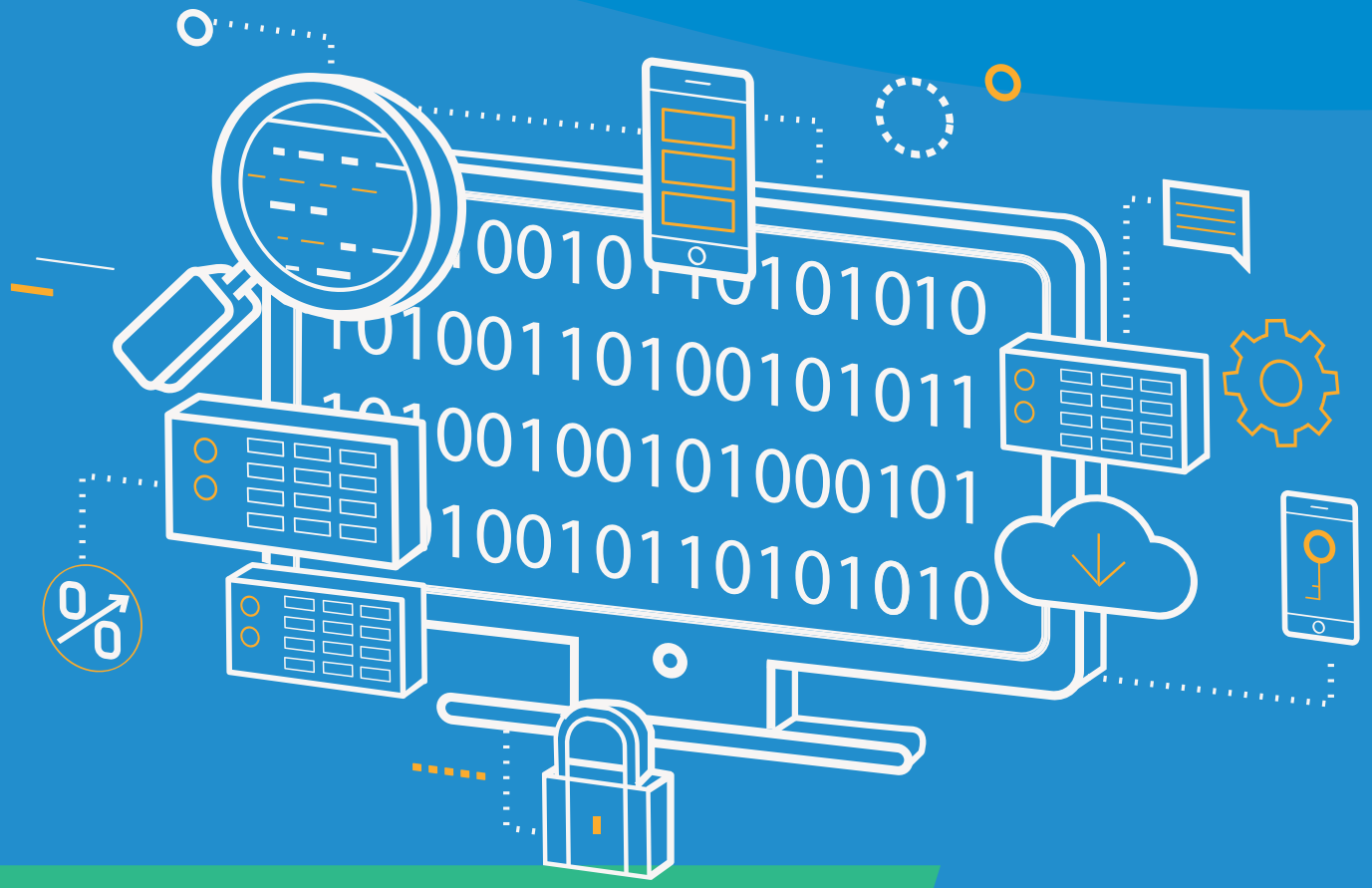
goanywhere
by HelpSystems



DMZ Gateways: Secret Weapons for Data Security

Executive Summary

Exchanging files with customers and trading partners is commonplace in today's global economy, but keeping that data secure remains a difficult challenge. Add to that the various compliance regulations governing data security, including PCI DSS, HIPAA, SOX, GBLA and more.

A common approach for protecting internal/private networks is for companies to install file sharing services (e.g. FTP/S, SFTP, HTTP/S servers) in a public zone for trading partners to access. When those servers and files leave the safety of the private network, however, companies then risk the exposure of those services and data to outside attacks.

This white paper will address the following questions:

1. Why is it dangerous for companies to store FTP servers and other file services in the DMZ?
2. How does incorporating a gateway into the file transfer process provide better protection for sensitive data?
3. How do gateways keep an organization's private network insulated from external breach?

DMZ for Staging Files

DMZ stands for demilitarized zone, and it's the neutral network that resides between the Internet and your company's private network. The DMZ is provisioned with a front-end firewall that limits inbound Internet traffic to certain systems within its zone. On the back end, another firewall is placed to prevent unauthorized access from the DMZ into the private network.

An organization's DMZ typically contains web servers, FTP/S, SFTP, and HTTP/S servers, as well as other services it wants to make available to its customers and trading partners. To serve their purpose, these services need access to the data files that will be shared with partners.

The DMZ serves as a staging area between an organization's private network and Internet. In order to share a document with a trading partner, an internal program or employee would first copy the file from the private network onto a server in the DMZ. The partner could then download the file from that server using an approved protocol like FTP/S, SFTP or HTTP/S.

When trading partners need to share documents with the organization, they would upload the files to a server in the DMZ. Later, an internal program or employee would scan for the files on that server and pull them into the private network.

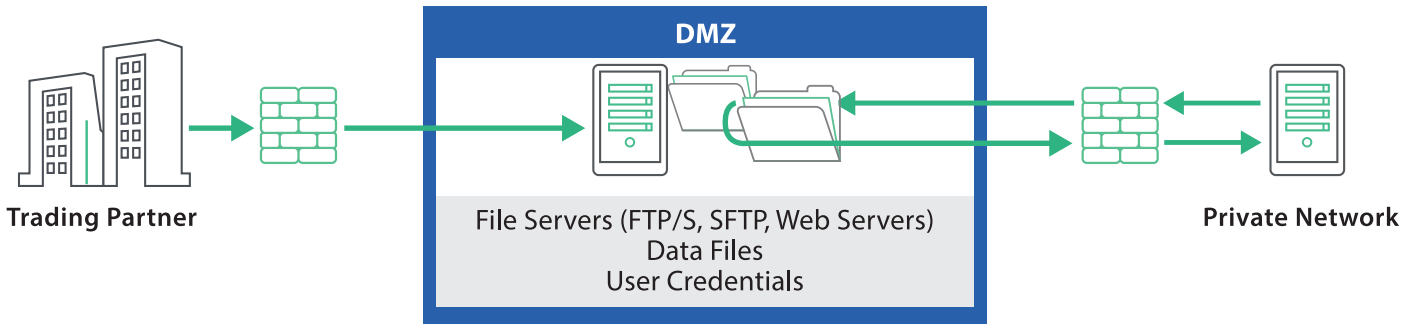
The DMZ often serves as a staging area between an organization's private network and Internet.

Dangers in the DMZ

While many organizations exchange files using this process, staging files in the publicly accessible DMZ makes them vulnerable to a variety of dangerous exploits.

- If attackers gain entry to a file server in the DMZ, they may be able to access sensitive trading partner files that were placed there. These files could be downloaded and their contents could be exposed by the attacker. Even encrypted files may be at risk to sophisticated attackers if the keys or passwords can be compromised. This concern is causing an increasing number of compliance auditors to prohibit data storage in the DMZ, encrypted or not.

- When the file sharing services are in the DMZ, then any user credentials, certificates, etc. needed for authentication are likely maintained there too, which makes them more vulnerable to attacks.



An increasing number of compliance auditors prohibit data storage in the DMZ, encrypted or not.

- Also at risk is the file sharing software itself, especially if it can be administered from within the DMZ. For example, an attacker could create a "back door" user account into an SFTP server through its admin console. This seemingly "legitimate" user account could then be used by the attacker to gather sensitive data files over an extended period of time. Audit logs for the software could also be manipulated if they are stored in the DMZ, erasing the attacker's trail.

An organization may react to these threats by moving its file sharing services (e.g. FTP/S servers or SFTP servers) and sensitive data files from the DMZ into its private network. However, the private network's inbound ports would traditionally need to be opened, which in turn creates an entirely new set of potential exposures and compliance issues.

Consider any organization that processes or stores credit card information, for example. Those companies must meet PCI DSS compliance standards that specifically "prohibit direct public access between the internet and any system component in the cardholder data environment."

So, if keeping file sharing services and shared files in the DMZ is dangerous, and allowing access to the private network through inbound ports is strongly discouraged, what other options are available?

A Better Solution: DMZ Gateways

DMZ gateways solve these security concerns by allowing an organization to move file sharing and other public services from the DMZ into the private network without having to open inbound ports. With this approach, data files also remain safe in the private network since they no longer need to be staged in the DMZ.

The gateway software, which should be installed on a hardened server in the DMZ, typically includes two proxy services. Its reverse proxy service will handle inbound requests from trading partners. The second service will be a forward proxy for handling outbound file transfer requests from internal employees and systems.

Reverse Proxy

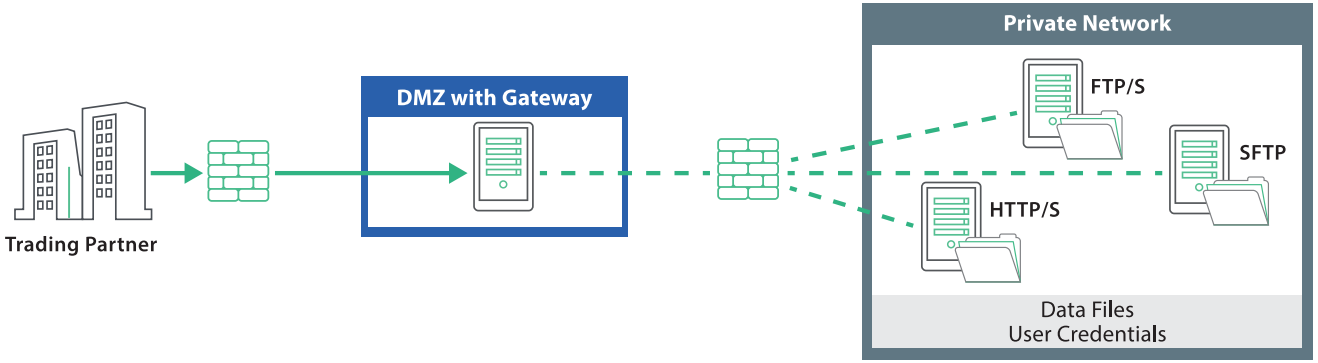
As a reverse proxy, the gateway masquerades as the file sharing services. When trading partners need to exchange data with your company, they would connect to the gateway instead. The gateway would then bind those requests to the appropriate back-end services in the private network.

It's important to note that adding a gateway will not affect your trading partners since they will be able to connect using the same protocols (e.g. FTP/S, SFTP, HTTP/S, etc.) and ports they've always used. This partner transparency will greatly minimize the gateway's implementation time and costs.

Forward Proxy

network and making any connections needed to external servers. This will allow an organization to more easily control these requests through its firewall.

A gateway installed in the DMZ reduces the likelihood of a security breach.



For example, a company may require that any FTP/S or SFTP file transfer requests from within the private network must pass through the gateway's forward proxy. The firewall rules could be configured to allow only the gateway's address (IP and port) for FTP/S or SFTP traffic, blocking all other addresses from performing those requests.

The internal users would specify the gateway's proxy address within their file transfer client software. When a user initiates a file transfer, the gateway would be passed the request and would then serve as the "middle man" between the user and the external server.

Keeping Inbound Ports Closed

The gateway should interact with the company's private network in the most secure way possible. A properly designed gateway will come with an additional component (i.e. service broker) that is installed in the private network. The service broker will communicate with the gateway in the DMZ over a proprietary control channel, keeping inbound ports closed into the private network.

The gateway uses the control channel to alert the service broker when a trading partner wants to initiate a file exchange. The service broker then connects to the appropriate backend service and creates a new outbound data channel through which the data exchange will be conducted. Any data channels needed are opened from the back-end services and through the gateway, again requiring no inbound ports.

Gateways Streamline File Transfers

In addition to the security risks associated with storing files and credentials in the DMZ, file transfers can be a time-consuming process for an organization's programmers who are writing scripts to help manage those transfers.

For example, consider a company that has a SFTP server installed in the DMZ. Trading partners upload files to this SFTP server throughout the day. One of the company's programmers has written a script that repeatedly scans a folder on the SFTP server every few minutes for new files. If files are found, the script then moves the files from the DMZ into the company's private network.

This scenario is typical, but definitely not foolproof. Here are a few of its potential issues.

- If the script fails to run, the files will remain in the DMZ, leaving them vulnerable to attacks.
- If the script lacks good error reporting or alerts, the company does not immediately know when a problem occurred.
- If the company adds additional trading partners, new scripts have to be written and maintained by a programmer, costing the company more time and money.

Conclusion

Even when files are encrypted and transferred through a secure protocol, data is still at risk if files, file servers and user credentials are stored within the DMZ.

A gateway removes that risk because it facilitates file transfers directly between trading partners and organizations without allowing direct access to an organization's private network.

As critical data breaches continue to make news, many organizations are searching for better ways to keep data secure and meet the compliance regulations of their industries.

By incorporating a gateway into the managed file transfer process, not only can internal staff's time and effort be redirected, customers and trading partners can feel confident that the files they exchange with organizations equipped with a gateway will be safe.

Gateways both improve security and streamline file transfers since files do not need to be staged in the DMZ.

goanywhere
by HelpSystems

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.

ga-gd-0221-r2-gm