eFolder White Paper: Three Network Security Tools to Block Dropbox in the Workplace

December 2014

Introduction

Bring your own device (BYOD) has been on the rise as employees bring the products and services they use at home into corporate environments. While many organizations have wholeheartedly embraced this notion — witness the number of tablets teeming in offices around the world as an example — BYOD poses a significant threat when the applications that employees bring into the office are not secure enough to handle sensitive corporate data.

Dropbox is a prime example of BYOD gone wrong. Though Dropbox is a great solution for consumers who want to bring their photos, music, and more wherever they are, it is ill-suited for sharing important and sensitive corporate information. The free version of Dropbox, for example, does not allow shared links to be protected with passwords, expiration dates, or download limits. Dropbox usage in the workplace poses serious risks of data theft, data loss, lawsuits, and more.

Though the dangers of Dropbox to corporate information are alarming, consumers continue to adopt and bring Dropbox into the workplace in increasing numbers. Therefore, it is imperative that business owners understand the different methods they can use to block employees from using Dropbox at work. This white paper discusses three network security tools — manual firewall configuration, next-generation firewalls, and DNS configuration — administrators can utilize to block Dropbox and other consumer-grade file sharing services.

Manual firewall configuration

At the bare minimum, system administrators looking to stop Dropbox usage in the workplace should ensure corporate firewall appliances are configured to block work machines from reaching Dropbox's servers. In doing so, system administrators can block employees from directly accessing Dropbox on computers and devices connected to the corporate network.

Before going into detail about this method, it is worth discussing how firewalls work in general. Imagine that a busy city, like New York City, represents the Internet. Lines of traffic traveling across town represent streams of data, such as Dropbox usage or Netflix streaming. Just as cars travel on streets, data travels along ports. To continue the analogy, cars that need to get to a specific destination need to take a route to that destination; similarly, for data to reach a specific server, the data needs to be able to reach the IP address associated with that server.

If the police block, say, the Brooklyn Bridge, a driver who normally uses that bridge would be forced to take a different set of streets to reach his or her destination. An important aspect of Internet traffic, though, is that it only travels on a specific route — it cannot decide to take a different path if necessary. As a result, if an IT administrator blocks a specific port (street) used by an application like Dropbox, Dropbox would no longer be able to send or receive data. IT administrators can also prevent data traffic from reaching destinations (e.g., Dropbox's servers) by blocking the IP addresses associated with those servers. Manually configuring a firewall therefore involves blocking certain ports or IP addresses to prevent data from reaching its intended destination, thus rendering an affected application, such as Dropbox, unusable.

Dropbox uses ports 80 (HTTP) and 443 (HTTPS) to transmit data between its servers and users' computers, but blocking these ports is not a desirable option because these same ports are used by browsers to access the Web. As a result, IT administrators who want to manually configure their corporate firewalls to block Dropbox should block all of Dropbox's IP addresses. These addresses are as follows:

DROPBOX (NET-199-47-216-0-1)	199.47.216.0 - 199.47.219.255
DROPBOX (NET6-2620-100-6000-1)	2620:100:6000:: - 2620:100:600F:FFFF:FFFF:FFFF:FFFF:FFFF
DROPBOX (NET-108-160-160-0-1)	108.160.160.0 - 108.160.175.255
DROPBOX-CORP (NET-205-189-0-0-1)	205.189.0.0 - 205.189.0.255
DROPBOXCORP (NET6-2620-C6-8000-1)	2620:C6:8000:: - 2620:C6:8000:FFFF:FFFF:FFFF:FFFF:FFFF
DROPBOX (NET-209-99-70-0-1)	209.99.70.0 - 209.99.70.255

IT managers who block Dropbox's IP addresses through the corporate firewall can prevent users from syncing files within the Dropbox application, even if it's installed on their local machine, and from reaching the Dropbox website.

A second way system administrators can manually configure firewalls is by deploying a Group Policy preventing the installation of Dropbox on work machines. Group Policies control what users can and cannot do on a computer system, and they can be edited on a per-user basis. The IP addresses above, along with the information below, can help an administrator create a Group Policy:

- **Network Ports (Default)**
  - HTTP – TCP 80
  - HTTPS – TCP 443
    - **NOTE:** by blocking TCP 443, Dropbox is crippled and cannot perform any sync functions, as it's required to do so over a secure connection.
  - HTTP – TCP 17500 (LAN Sync)

- **Domain Names**
  - Dropbox.com
  - amazonaws.com — Amazon's web services and cloud computing platform
  - akamaitechnologies.com — a content-delivery network used by companies like Adobe
  - softlayer.com — a dedicated server, managed hosting and cloud computing provider now owned by IBM

- **Application Name**
  - Dropbox.exe

IT administrators should take care to note that Microsoft's Group Policies were designed for Windows-based computers, and that separate configuration instructions may be needed to ensure Group Policies apply to Macs and other non-Windows devices.

Regardless of which manual firewall configuration option an IT manager chooses, there are a couple important limitations to this approach. First, manual firewall configuration can effectively block access to Dropbox from computers and devices connected to the corporate network, but many personal mobile devices employees carry into the office that are not connected to the corporate network, such as their mobile phones, can still access Dropbox over a cellular network. Additionally, IP address blocks can be circumvented through proxy servers (which is more likely to occur on a device not provisioned by IT, such as an employee's personal iPad).

Next-Generation Firewalls

Rather than resorting to manually blocking IP addresses and websites using a traditional firewall, companies can also use a "Next-Generation Firewall" (NGFW) to precisely monitor and block Internet traffic.

"Next-generation firewalls" (NGFWs), named so because they are far more powerful than traditional firewall appliances, are at the heart of advanced network security appliances created by companies such as Palo Alto Networks, Cisco, and Dell SonicWALL. Traditional firewall appliances sit at the edge of corporate networks, enforcing specific filtering policies to keep harmful applications and malware at bay and prevent employees from accessing inappropriate sites. Where next-generation firewalls advance far beyond their forebears is in their intelligence.

Normal firewalls must rely on administrator-specified rules to block specific IP addresses and domains. This is why proxies can be used to sidestep manually configured firewalls; they essentially allow users to take secret side roads to reach their destination, even if the main roads are blocked. NGFWs, however, can inspect individual packets of data to identify where they are coming from or going to. Next-generation firewalls can also be used to determine who is using specific applications (e.g., Dropbox) and provide IT administrators with granular control of applications and users. In short, NGFWs are automated tools that can identify precisely what is going on in the network at any given time and can act on this intelligence.

Many corporate firewalls also have a content filtering enforcement agent that goes on company-configured notebooks to enforce filtering policies when machines are outside the corporate firewall. As a result, IT administrators can discourage Dropbox use by blocking it on company notebooks even when employees take these devices home.

Next-generation firewalls are certainly effective on the PCs they control. That said, they can be expensive and complex to configure. Still, using hardware network security appliances with NGFWs is much more effective than manually configuring traditional firewalls as outlined earlier.

DNS configuration

There is a third option for system administrators who want additional protection on top of what a traditional firewall offers. Utilizing a cloud-based network security solution such as OpenDNS can ensure employees connected to a corporate network do not access non-secure or dangerous websites and applications.

To understand what OpenDNS and similar services do, imagine that DNS (Domain Name Service) is a phonebook for the Internet. Just as a normal phonebook allows people to look up names and find corresponding numbers, DNS lets Internet users navigate to an easy-to-remember URL (e.g., http://www.google.com) and redirects them to the actual IP address of the server they're trying to reach (in Google's case, this IP address is 74.125.224.72). OpenDNS and other tools essentially work as an intelligent "layer" on top of the traditional DNS system, analyzing the traffic flowing through the network and giving administrators the ability to monitor and filter traffic as needed.

In the case of an IT manager looking to block Dropbox, he or she could configure OpenDNS or another similar tool to block all traffic involving Dropbox's website or desktop application. Since OpenDNS and other DNS services work in concert with firewalls, IT administrators can leverage the capabilities of both DNS services and firewalls. Firewalls can perform critical tasks, such as port filtering, IT address filtering, NAT/PAT translations, and more, while OpenDNS (or another DNS service) can take care of content filtering to block Dropbox and other non-secure applications.

Cloud-based network security solutions are excellent tools for monitoring and controlling traffic on a corporate (or non-corporate) network, but using them to block a popular application such as Dropbox may not go over well with some employees. Savvy users may simply adopt other insecure consumer-grade file syncing products, such as Microsoft OneDrive, or may transfer important files to a personal USB drive — which could amplify the very security risks business owners want to avoid.

Conclusion

It is important to take a step back and understand why business owners should go through the trouble of blocking Dropbox in the workplace — the opportunities for sensitive corporate data to leak abound and pose serious risks to companies' livelihoods. Though the benefits of file sharing for collaboration and flexibility are undeniable, every company also considers it a priority to safeguard important data, and rightfully so. It is therefore imperative for small- and medium-sized companies interested in giving their employees the flexibility of file sharing and syncing to adopt a secure, business-class solution.

Business-class file sync solutions such as eFolder Anchor are as easy to use as Dropbox, but are substantially more secure. Anchor includes robust file syncing and sharing options and is supplemented by features that business owners and IT administrations can use to keep track of their data.

Ultimately, business owners have a choice. One option is to leave their sensitive data up for grabs by letting their employees use non-secure, consumer-grade file sharing services. Alternatively, businesses can secure their data while still enabling the sync and share features that will make employees productive. Continued use of services such as Dropbox is evidence of the former, inferior approach. True business-class solutions such as Anchor accomplish the latter, making both users and IT managers happy.

Corporate Headquarters
2340 Perimeter Park Drive, Suite 100, Atlanta, GA 30341 ▪ 678-888-0700 ▪ www.efolder.net