Optimizing ownCloud Security

Tips & tricks for the security conscientious

A recent study by Harris Interactive found that 38% of those surveyed admitted to using a file sharing solution that is not approved by IT leaving the organization vulnerable. Adding to security concerns over 80% of employed adults use at least one personally owned electronic device for business.[1] The key towards closing this security gap is to provide an IT monitored and approved file sharing solution that employees want to use.

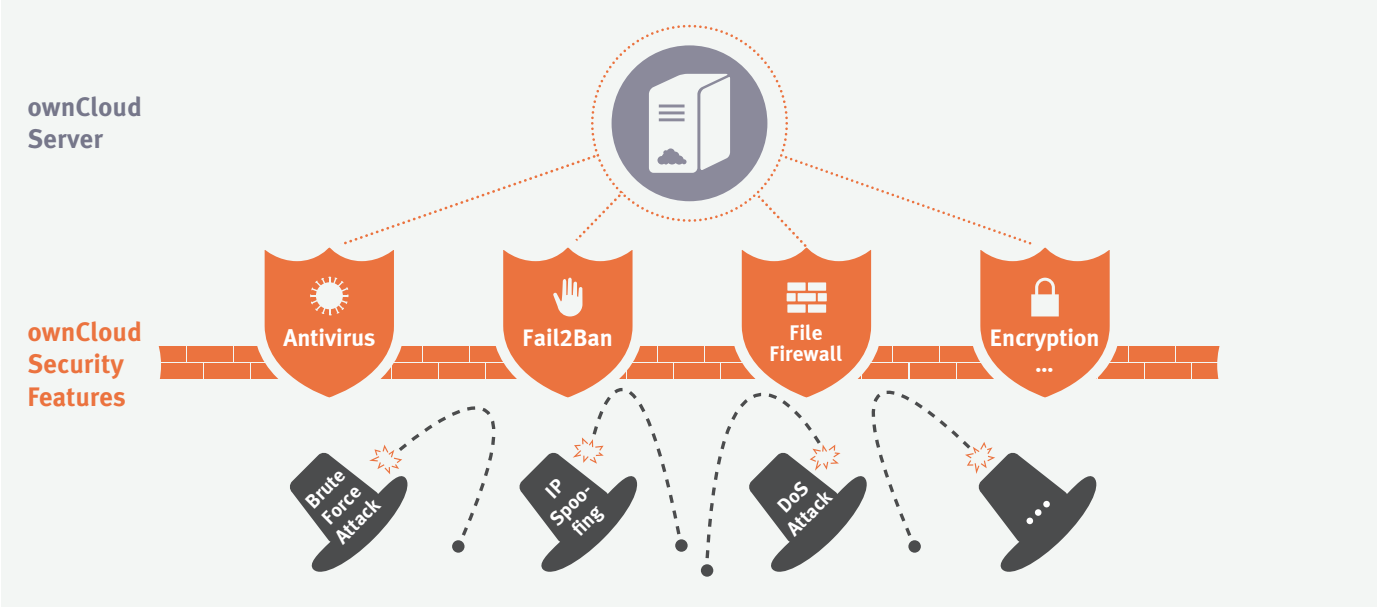

Figure 1: ownCloud security features help you ensure that data stored on the ownCloud server remains secure.

ownCloud's unique approach to file sync and share is inherently more secure because you keep your files where they were published which means that your most important assets stay in your data center and within your IT department's governance. At the same time ownCloud provides the usability and productivity users demand.

ownCloud Security features

Unlike consumer cloud-based services, ownCloud's server enables IT to protect and manage every element associated with ownCloud onsite – from file storage to user provisioning and data management. The server provides a secure web portal through which the entire system is controlled by the administrator, providing the ability to enable and disable features, set policies and manage users.

When sharing files, security is of utmost importance and that's why ownCloud takes security seriously. We use only documented APIs to integrate secondary storage devices where your hardware and governance policies are maintained. Further we can integrate with your existing authentication services without having to store your user credentials. Lastly, we've taken the extra step to ensure there are no gaps in security using encryption to secure files in-transit or at rest in ownCloud storage.

"ownCloud makes safeguarding your files easy to implement by fully leveraging industry standard protocols and your existing security infrastructure without sacrificing usability."

Frank Karlitschek,
ownCloud Chief
Technology Officer

[1] http://www.mobileauthenticationtoday.com/byod-swot-and-statistics/

Keep your data where it is
ownCloud is hosted in your data center – or in a third-party data center of your choosing – on physical, virtual or private cloud servers.

Give IT complete control
IT controls and manages ownCloud. Administrators define security policies down to the file level, provision users and groups, monitor activity logs and overall system health, and manage usage and quotas – all from ownCloud's admin interface.

Leverage existing technology investments
ownCloud integrates easily with enterprise file sharing and storage technologies, governance workflows, security systems and monitoring tools.

Automate user authentication
Built-in wizards allow IT to integrate ownCloud with Active Directory or LDAP. Single Sign On (SSO) is also supported. Shibboleth, a SAML-based authentication is integrated with ownCloud's web-frontend as well as the ownCloud mobile apps and desktop clients. As users are managed by those services, ownCloud automatically acquires and implements the associated authentication.

Restrict access to data at multiple levels
User or file-level permissions can be defined when and where files are shared. Access expiration dates and restrictions can be set at multiple levels. Plus, administrators can use File Firewall to create rules that control access to ownCloud servers based on user connections, time intervals, geographic locations and more. And, with CRUDS, admins can overwrite sharing if necessary.

Ward off viruses with antivirus scanning
Uploaded files are scanned with ClamAV, preventing the potential for automated distribution of infected files. Or, with minimal customization, external virus scanners may be used to scan files as they arrive on the server.

Enable full auditability
Not only does ownCloud allow you to control each user's permissions, but it also enables a full audit trail—allowing you to understand how, when and where data is accessed and shared. Two separate apps enable admins to log account level activities such as logins to ownCloud as well as what users do with files on the server. This provides admins the basic information they need for compliance reporting and auditing of ownCloud usage and the tools to actively follow file sharing activities.

Configuration Best Practices

In addition to ownCloud's built-in security measures, you will also want to ensure that your ownCloud environment follows recommended security practices to avoid opening vulnerabilities. These common sense practices will optimize security:

Avoid firewall exposure
Opening ports in your firewall for data transmission should be carefully monitored and applied. Open only those ports truly required to reduce the potential attack surface, and ensure that each port that is open is monitored; an open, obscure, unmonitored port is the biggest threat. For most implementations ownCloud only requires a single port be opened – Port 443 for TLS/SSL traffic.

Secure shared memory
As shared memory can be used in an attack against a running service, it is important to secure it against an attack by using fstab. How fstab is utilized will vary by operating system but as an example you can create the following entry in /etc/fstab to secure shared memory in a Ubuntu 12.04 LTS system:

```
tmpfs /dev/shm tmpfs
defaults,noexec,nosuid 0 0
```

Secure Shell (SSH)
The best way to secure SSH is to use the public/private key-based login. However, if you need to use the user name and password method, simply disable root and change the port it uses to reduce the attack surface.

Protect servers by limiting access to only the admin group
This seems obvious but is often overlooked. If you have ownCloud web servers that will live outside your firewall, make the potential attack surface as small as possible by limiting access to only the admin group.

Harden network using sysctl settings
Sysctl is an interface for examining and dynamically changing parameters in the BSD and Linux operating systems. This is a sample list of things which can be addressed by modifying the sysctl.conf:

1. Network configuration to limit IPv4 traffic
2. Network configuration to limit IPv6 traffic
3. Turn on exec shield protection
4. Protect against common 'syn flood attack'
5. Turn on source IP address verification
6. Prevent the use of spoofing attacks against the IP address of the server
7. Log several types of suspicious packets, such as spoofed packets, source routed packets, and redirects.

Disable OpenDNS recursion and remove version info - Bind9 DNS
Although not common, you may occasionally host the DNS Server on the same system as the web server. In this case, make as little information about your environment available to a potential attacker as possible. Simply modify your named.conf file in the options section to NOT display this information.

Prevent IP spoofing
This is a protection that prevents your network from being the source of a spoofed (i.e. forged) communication, which is mostly used on DoS attacks. Turn on rp_filter or reverse path filtering using the following command:

```
echo 1 > /proc/sys/net/ipv4/
conf/all/rp_filter
```

This will create the default interface and help prevent spoofing by making sure that the packet source address is routable through the interface in which it was received, or in an alternative setting, routable through any of the available instances. This is why packets which have a source IP that is not routable are dropped.

Harden PHP
While some items are completed with your software vendor, there are some actions you can consider when setting up your server(s).

- Review documented items and tips from php.net which can be found at http://php.net/manual/en/security.php
- Consider the PHP Suhosin plugin for your installation to help secure PHP in a manner outlined at http://www.suhosin.org/stories/feature-list.html
- Restrict Apache information leakage by minimizing the information about your system available to a potential hacker by removing the Server Version Banner.
- In the https.conf file find the following entries and change them to the following:
  ServerTokens Prod
  ServerSignature Off

Installation of ModSecurity
ModSecurity is an application firewall that can be installed with Apache, IIS, and Nginx to give administrators tighter controls. It includes more granular logging options, real time monitoring of traffic with alerting, and more. ModSecurity is designed specifically to reduce the attack surface of your web application by using heuristic filters that detect malicious patterns or by whitelisting required resources and only using values that align.

Install Mod_evasive
This is a module designed specifically to help prevent HTTP DoS or DDoS attacks. You may configure the tool to avoid false positives while blacklisting suspected IPs which may be generating scripted attacks against your ownCloud instance. Rules may be implemented to protect against scenaris such as:

- Requesting the same page more than X times per second
- Making more than X concurrent requests on the same IP per second
- Making requests while blacklisted (blocked)

Monitoring of logs using tools like Fail2Ban
You can use a log monitoring tool like Fail2Ban to scan the Apache logs for suspicious activity which dynamically updates your firewall to reject traffic coming from suspicious source IPs. This is a configurable tool that will assist in reducing the risk associated with a brute force attack on your system.

Intrusion detection
With tools like PSAD, you can analyze iptables logs for suspicious activity like port scans and other questionable traffic and take a proactive approach to attacks or preemptive scans on your system.

Installing with SELinux or AppArmor
These technologies are designed to help secure your system by setting context around file and network access, and help minimize the damage that could be done should someone gain access to your system. Often SELinux or AppArmor are simply turned off as they can make installing and working with applications and database difficult if not setup correctly.

Monitor logs
To stay current on the health of your system, we encourage the monitoring of key logs including the ownCloud log file along with system logs and Apache/web server logs. Consolidating these using a tool like SPLUNK makes it easy to create security dashboards for your systems, and understand their status in real time.

As part of the ownCloud deployment service, an ownCloud technical consultant can assist you in setting up this level of monitoring to help secure your system.

TLS/SSL
This seems obvious, but no security conversation would be complete without the strong recommendation that all communication be secured using TLS/SSL.

Antivirus
We strongly recommend you enable ClamAV, the antivirus application available in the ownCloud Enterprise Edition. This will help ensure that infected files are removed and can not reach your users.

As part of the ownCloud Deploy service package, ownCloud consultants can help you configure the specifics. Contact us at owncloud.com/contact to schedule a consultation.

With over 1.6 million users across the globe, ownCloud gives users the opportunity to easily sync and share files while providing administrators the control and governance required by existing security policies. Uniquely offering both control and access, ownCloud offers enterprise-grade file sharing that protects sensitive data onsite, under IT's control.

For detailed information about ownCloud and to test drive ownCloud within your organization today, visit www.owncloud.com.

ownCloud, Inc.
57 Bedford Street
Suite 102
Lexington, MA 02422
United States

www.owncloud.com/contact
phone: +1 (877) 394-2030

www.owncloud.com

@ownCloud
facebook.com/owncloud
gplus.is/owncloud
linkedin.com/company/owncloud