

Securing Dedicated and Virtual Private WordPress Servers with Dome9

A Whitepaper by Dome9 Security, Ltd.



Executive Overview

Security is one of the most intricate and complex areas of IT, so it's no wonder that many are at a loss when they try to protect their WordPress websites and servers. It's easy to overlook a number of scenarios, which can leave your system vulnerable to security threats. What's more, when you're dealing with a WordPress site that's hosted or in the cloud, your challenge is compounded by the fact that you neither own nor manage the infrastructure. Fortunately, Dome9 makes it easy to secure your WordPress websites and servers.

WordPress is one of the leading website platforms, with more than 50 million deployments on shared, dedicated, and virtual private servers. There are deployments of both professional and personally run websites, large and small, with advanced functionality and social media capabilities.

Despite its popularity, WordPress and many web platforms like it are highly susceptible to security threats and are vulnerable to various forms of attacks. WordPress administrative console, for example, is often exposed on well-known internet ports (80 and 443). While administrators and developers use these channels to connect to and manage their web applications, they're also exploited by attackers. With WordPress, security is relegated to a simple username and password authentication over a secure channel (e.g., SSL). That is the only level of protection and, most often, the only mechanism that stands between potential malicious hackers and the WordPress websites.

Dome9 takes securing access to your WordPress website to the next level. It enables complete automation of safe and secure access to the WordPress administrative console. The solution closes down administrative port 443 and eliminates the potential for brute-force attacks by hackers. Dome9 does this by providing a centrally managed security layer around your WordPress servers, limiting secure access only when and for whom its needed. The approach is flexible, manageable, and maintainable; it is platform-independent and is supported on dedicated and virtual private servers.

Setup of Dome9 is accomplished in just a few simple steps and does not require knowledge of advanced security concepts. Dome9 centrally manages secure access for multiple WordPress websites hosted in either dedicated environments or virtual private servers. The solution creates a virtual security layer around the WordPress administrative and development interfaces, providing greater, more efficient security management.

WordPress Security Challenges

There are many vulnerabilities within WordPress websites, as with just about every web application. Securing access to the WordPress administrative console is the easiest and yet frequently most overlooked area. The current approach to WordPress security relies on username with password transmitted over Secure Sockets Layer (SSL). Hackers need only guess the username and password, impersonating administrative accounts, and gaining unrestricted access to and control of your system. Various outdated and unmaintained plugins, which you may have installed on your WordPress site, could also have numerous vulnerabilities and be susceptible to security threats. All of this may compromise the security and safety of your WordPress site and server.

Attackers often utilize a brute-force attack or exhaustive key search, wherein a hacker or a bot systematically checks all possible combinations of a username and password until the correct one is determined. The attackers will attempt to break into and gain complete access to your WordPress website by sending malicious requests carrying exploits for various vulnerabilities of the software running on your hosting servers as well as a number of custom plugins installed on your site. A malicious attacker may attempt to obtain your cookies and, in some cases, authentication headers. Upon successfully stealing such cookies, the hacker can use them to impersonate your account and gain complete access to your WordPress environment.

An important caveat is that security itself isn't necessarily the sole solution. There are also many management issues associated with security. Most WordPress servers are hosted outside traditional data-centers. They are often hosted by third-party providers, which can lead to a number of problems. First, you have less control of the infrastructure and limited options for providing security, especially with out-of-the-box capabilities. Second, you are generally constrained in your options to what the provider has available. Third, our security becomes overlooked because you tend to rely too much on your hosting provider because you assume that the provider has the responsibility for ensuring security for your server and website. Typically, your choices are most often limited to manually enforcing SSL, and a combination of tricks and plugins. In most cases, such approaches are cumbersome, hard to maintain, and still leave a number of holes and vulnerabilities.

Some of this complexity, investment of time, and extra resources lead to a hodgepodge of custom plugins yielding a less-than-optimal security solution. Approaches for secure and safe access to the administrative console of the WordPress website, in many cases, are not as scalable, and may not be able to adequately support medium to large WordPress server installations, which require secure access by a number of administrators and developers. All of these factors and circumstances may enable hackers to take complete control of your WordPress website and cause significant damage.

Introducing Dome9 Security

Dome9 is a first-of-its-kind cloud server security management service that provides protection for hosted, cloud, and Virtual Private Servers (VPS), including those supporting WordPress. Its solution provides an efficient and effective dedicated virtual security layer on top of your WordPress website and server to secure access and prevent unauthorized hackers from attacking and accessing your WordPress site. Dome9 eliminates the possibility and application of various security hacking techniques such as guessing usernames and passwords. It secures the administrative console within WordPress, otherwise left vulnerable to attacks.

With Dome9 security, you are equipped with safe and secure on-demand access using time-based controls for you and your WordPress developers and administrators. In addition to securing access to your WordPress administrative console (i.e., the application running on your server), Dome9 also secures the underlying server itself. That's because Dome9 can manage secure access and firewall policy for port 443 – the administrative port that the WordPress administrative console uses, as well as any other port on your server. Dome9 secures other ports too, including RDP (Remote Desktop Protocol), SSH, MYSQL, and more, which are frequently left open by administrators to connect, manage, and operate the server itself.

Dome9 service provides an array of capabilities – many of which will be explored in this paper, including Secure Access Lease™ Technology, multi-platform management, secure access lease invitations - all with fully centralized and scalable controls. These features eliminate the possibility of a brute-force attack on the WordPress servers and prevent hackers from seizing control of your websites.

Getting Started with Dome9 for WordPress Security

Securing your WordPress server and website with Dome9 is fast and easy. First, sign up for a Dome9 account at www.dome9.com. Then connect to your WordPress server via SSH (Secure Shell), Remote Desktop, or another remote connection utility, open a browser, and login to your Dome9 account. Follow the onscreen instructions to install the Dome9 agent for your server. The whole process should take under five minutes.

Now that you've created an account and installed the agent, you can immediately begin managing secure access for RDP, SSH, as well as other ports within Dome9 Central – the web-based management console for Dome9. However, one important step remains in order to secure the WordPress administrative console access on port 443.

Ensure SSL is configured on the server hosting the WordPress website by setting your WordPress server to accept administrative access only through port 443. You can accomplish this by installing the "SSL Administration" plugin. All communication and cookies are encrypted and safe upon configuring these settings. Additional information describing this procedure is available here: http://codex.wordpress.org/Administration_Over_SSL.



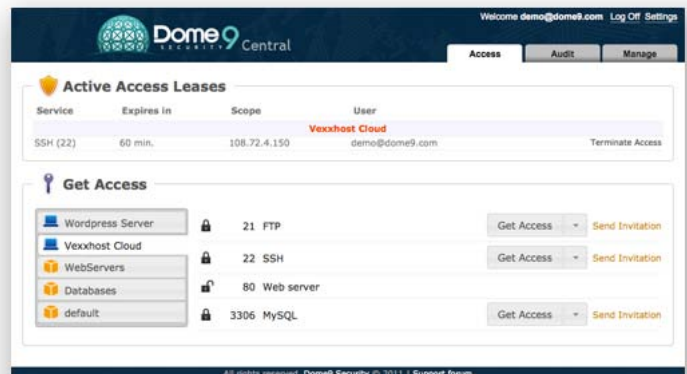
You can secure additional WordPress websites by adding them to Dome9 Central and repeating the process at any time. Upon successful installation of the security agent, select "Service" section and click "Add Service". In the dialog window, enter the name of your WordPress server, a short description, port number (443), choose TCP protocol, and finally select "Open on Demand" from the drop down list. This automatically configures your WordPress Server to have port 443 closed by default, and only open it when you explicitly request access through the Dome9 Central console.

With your WordPress Server secured, anyone who's not authorized that tries to access the WordPress administrative console will get a "Not Found" response from the server (an HTTP standard response code 404). To gain administrative access to your WordPress website, you simply first login to the Dome9 Central, select the WordPress website you would like to access, and click the "Get Access" button. The Dome9 security agent will then automatically open port 443 on your WordPress server. The channel and port will only be open for your specific Internet Protocol (IP) address, and access will be available for one hour by default. You can adjust the access time-window via the "Get Access" drop down list. Note: only you can see and access the WordPress administrative console since the secure access channel you created is open only for your specific IP address.

If there is a third party administrator or developer for whom you would like to enable administrative access to your WordPress website, you can easily do so by sending a secure access invitation by clicking on the link labeled, "Send Invitation" next to the "Get Access" button.

Key Features and Benefits

There are three primary benefits to Dome9's secure access service. It provides an efficient and effective means to secure your WordPress websites and servers that's easily expandable to support your other database and application servers across all your clouds.



1. **Simplicity that speaks for itself:** Security is no easy task. Securing the cloud, an environment you have far less control of, only exacerbates the problem. Dome9 provides a fast and proven approach to the automation and central management of security features, and enables flexibility, maintainability, and scalability. Best of all, Dome9 gives you a rock-solid, manageable front-line of defense that's far easier and more effective than plugins, custom hacks, and other options to harden security around your WordPress website.
2. **Security that scales:** Dome9 provides an elastic and secure solution. Its centralized management for WordPress security spans hosting platforms, allowing you to retain your security across clouds, and centralizing your WordPress and other hosting and cloud-based servers. Secure and safe access is granted on-demand when administrator or developer needs to perform certain tasks on your WordPress website. If no access is required, there is no attack surface because administrative ports on your servers are closed.
3. **Automation that can be trusted:** Dome9 provides time-constrained secure access to the WordPress servers only letting through requests made from your specific IP address. Thus, only traffic from your originating IP address is allowed to the administrative functionality of your WordPress site. You have the ability to send safe and secure invitations to a third party administrator or developer to gain secure access to your WordPress site. This is very helpful for both medium and large WordPress websites which have multiple administrators or developers.

In Summary

Dome9 Security is as elegant as it is simple, scalable, and non-intrusive. The cloud-based security provided via Dome9 is well-designed and easy to deploy and leverage. Its approach is flexible and extensible to other hosted environments and cloud infrastructures, and it provides great benefits with marginal security investment.

Cloud security offered by Dome9 provides the next level of protection for WordPress servers and sites. The solution is designed to manage and secure access to both virtual private servers, cloud, as well as dedicated WordPress deployments.

WordPress is a trusted and popular website and blogging platform. Its proliferation yields security weaknesses. You can take actions to eliminate security-related risks around it. If you are serious about protecting your dedicated or virtual private WordPress server, the first and most important step should be to secure it. Using Dome9 makes it fast and easy. Secure your WordPress server and site today, with Dome9.

Visit <http://www.dome9.com> today and try Dome9 for free!

About Dome9 Security

Dome9 makes security as elastic as the cloud with first-of-its-kind multi-platform cloud server security management. Available for the enterprise and hosting providers, Dome9 provides dynamic security policy control for Clouds, Virtual Private Servers (VPS), dedicated servers, and Amazon's EC2 Security Groups, across all major operating systems and service providers.



Copyright © 2011 Dome9 Security, Inc. All rights reserved. Dome9 Security, its logo, and other marks are registered trademarks of Dome9 Security. All other trademarks are the property of their respective owners.