NEXUSGUARD

White Paper

Mitigating SSL Attacks Without **Private Keys**

V2.1.1

Secure Socket Layer (SSL) is a protocol widely used to secure HTTP traffic between web servers and browsers. The protocol relies on public- and private-key encryption to ensure the safe transit of data across the network.

Unfortunately, stealthy DDoS attacks can also be initiated the same way. With reasonable know-how, an attacker can easily encrypt a DDoS attack that will evade mitigation efforts if the appropriate decryption key is not readily accessible to decode the attack.

In order for mitigation measures to be effective, a matching private key is required to decode attack communications and perform the necessary filtering by examining the packet headers. To do that, a DDoS protection service provider needs to hold the site owner's private key. After attack detection and the scrubbing process are completed, clean traffic, either re-encrypted or in plain HTTP text, can be routed back to the client's web server.

As such, the "key" to preventing encrypted SSL attacks is to have in place a proven system for ensuring the secure handling and agile management of private SSL keys. At Nexusguard, we understand the sensitivity concerns of private key holders, and, following the most stringent measures, have established the Nexusguard Secure Key Management Infrastructure (KMI) to keep private keys safe at all times:

- Complex Management – can manage millions of key encryptions
- Uncompromised Security Assurance - minimizes the need for human intervention to the greatest extent possible
- Data Availability - maintains high availability of keys for authorized users

(See our SSL Key Management White Paper for details about the inner workings and implementation of the KMI.)

While most clients trust Nexusguard to look after private keys, some — due to regulatory requirements or internal security policies — prefer to not turn over their private key to a third-party vendor. There are three mainstream solutions to address this concern and enable site owners to keep their private keys while handling and mitigating SSL-based attacks:

1. Additional on-premise hardware
2. A dedicated key server to generate session keys
3. A separate SSL key pair issued by certificate authorities (CAs) — the Nexusguard approach

1) The "box" approach

The site owner deploys on-premise hardware, including a module dedicated to storing the private key files. The site owner can directly import the files to the "box," or upload them through a vendor-provided portal. The key files are then stored and encrypted under another key on the dedicated appliance. When done, the box can decrypt packets of incoming traffic within the appliance and examine them to judge whether it is a DDoS attack.

This approach allows the decryption and examination of SSL traffic to be carried out in a private environment, thereby providing site owners with additional peace of mind. However, a major drawback is that, under enormous volumetric attacks, on-premise appliances can become traffic bottlenecks themselves. To accommodate high-traffic, volumetric attacks without having to hand over the private key, a site owner needs to leverage the immense scalability of the cloud offered by a DDoS service provider like Nexusguard.

2) The "key server" approach

This approach calls for storing the private key on a separate key server and running a software agent on the site owner's hardware behind the firewall. The cloud-based scrubbing centers serve as the proxy on behalf of the site owner, but have no access to the private key.

Every time a visitor requests access to the website, the cloud provider contacts the key server to decrypt a premastered secret from which the cloud provider derives a session key. With the session key, the cloud provider decrypts the SSL request sent by the visitor, and consequently, the service provider and the site visitor establish an encrypted channel.

Because the session key is short-lived and only protects one visitor's communications, it is not as sensitive as a long-lived private key. The decrypted traffic is analyzed and filtered over the cloud, while clean traffic is finally routed back to the web server, either re-encrypted or in plain HTTP text.

This solution requires the site owner to install an additional key server, and therefore involves upfront costs and extra deployment time. Also, the software has to be updated frequently in order to keep up with the latest cryptographic algorithms and encryption technologies. Another major drawback is that the key server may be overloaded during large-scale, volumetric attacks, while the loss of a premastered key can also cause a delay in decryption.

3) The Nexusguard Approach: a separate key pair signed by a trusted CA

This easy, yet highly effective approach uses two key pairs, one each for the Visitor-to-Nexusguard and Nexusguard-to-Server sessions. Specifically, the original pair, including the site owner's private key, is only used in the Nexusguard-to-Server session, so the site owner retains control of the private key.

To follow this approach, a valid SSL certificate[1] for the domain must first be installed on our cloud servers worldwide. To provision this certificate, we partner with leading certificate authorities (CAs) to authorize the site owner to issue certificates to Nexusguard — simply and at no additional cost.

The original web server's certificate is used for Nexusguard-to-Server requests, while the new Nexusguard-issued certificates are used to handle all Nexusguard-to-Visitor traffic.

To ensure maximum security, Nexusguard-issued certificates are signed by the world's leading SSL authorities, supported by all major browsers and devices, and trusted by 99.99 percent of the Internet universe. Moreover, Nexusguard-issued certificates use 2048 bit key encryption, thus boosting security for all 1024 bit certificate holders.

Due to the constraint that SSL requires its own IP address and that each of our data centers around the world needs to have a valid version of every certificate, we use multi-domain SSL certificates (MDC). This allows us to include multiple domain names within the same certificate and solve the IP shortage problem. Simply put, we use a single certificate to serve every one of the site owner's domains.

1 Only supports Domain Validated (DV) SSL Certification

The site owner's approval for using Nexusguard's custom SSL certificates is obtained via an API embedded in an email provided by our partner CAs. This gives the site owner the right to revoke the certificate at anytime. The SSL email authorization process consists of the following steps:

1. Nexusguard requests its CA to add the site owner's domain(s) to its existing MDC.

2. The CA sends an email to the site owner requesting approval for Nexusguard's application.

3. Once the site owner has approved the request, the CA issues Nexusguard a renewed MDC that includes the newly added domain(s).

4. The site owner can also opt for alternative provisioning, such as approving Nexusguard's certificate using a DNS txt record or going through the CA's URL verification methods.

When the MDC becomes effective, traffic can be encrypted and decrypted for scrubbing by Nexusguard. Clean traffic, which is re-encrypted with the web server's original SSL certificate, is then routed back to the original web server.

In between, the decrypted SSL traffic that passes through our mitigation services and VAS platform is scrubbed against all types of DDoS attacks, including network attacks (Layers 3 and 4), session attacks (Layers 5 and 6), application attacks (Layer 7), and business-logic attacks. While traffic is en route, the site owner does not need to surrender its private key to Nexusguard.

"Key" advantages of the Nexusguard Way

- Zero-cost, turnkey approach for keeping control of private keys while allowing Nexusguard to mitigate encrypted DDoS attacks
- No hardware/software installation, maintenance or updates
- SSL certificates are signed by leading CAs
- Site owner can revoke/replace Nexusguard's SSL certificate whenever desired at its sole discretion

Conclusion

With Nexusguard holding a separate key pair signed by a trusted CA, the Nexusguard approach is a turnkey, cost-effective and hassle-free solution for site owners who wish to retain their private key without having to install additional hardware or software. Other foreseeable problems, such as operator errors and hardware failures are also eliminated by opting for the Nexusguard solution.

To follow the Nexusguard way, a site owner only has to authorize the issuance of an SSL certificate to Nexusguard in order for it to generate CSRs (Certificate Signing Requests) for visitors to the original domain. Deployment is cost free and the site owner can revoke or replace certificates issued to Nexusguard at any time.

Site owners can rest assured that the original private keys are always under their control, while allowing Nexusguard to inspect incoming traffic, including encrypted traffic, against all DDoS threats.

White Paper

NEXUSGUARD

Founded in 2008, Nexusguard is the global leader in fighting malicious internet attacks. Nexusguard protects clients against a multitude of threats, including distributed denial of service (DDoS) attacks, to ensure uninterrupted internet service. Nexusguard provides comprehensive, highly customized solutions for customers of all sizes, across a range of industries, and also enables turnkey anti-DDoS solutions for service providers. Nexusguard delivers on its promise to maximize peace of mind by minimizing threats. Headquartered in San Francisco, Nexusguard's network of security experts extends globally.

Twitter twitter.com/nexusguard
Facebook facebook.com/NXG.PR
LinkedIn linkedin.com/company/nexusguard

nexusguard.com
contact@nexusguard.com

20150521-EN-A4