In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the December 2013 edition of In the Boxing Ring

This month, we discuss in detail the Network Box 5 **SSL Proxy**. Secure Sockets Layer (SSL), also known as Transport Layer Security (TLS), are cryptographic protocols which are designed to provide communication security over the Internet.

In this case, SSL/TLS is a protocol used to protect network traffic. It is commonly used as an option in such protocols as HTTP (HTTPS), SMTP (SMTP), IMAP (IMAPS), etc. The protocol is either used directly over a dedicated port (e.g.; tcp/443 for HTTPS, tcp/993 for IMAPS) or enabled mid-protocol (e.g.; CONNECT for proxied HTTP, STARTTLS for SMTP).

Network Box 5 includes a SSL Proxy security module that provides for identification, decryption, encryption, certificate validation, and protection of SSL network traffic. On pages 2-3 we describe, in detail, how this proxy operates.

On pages 4-5, we highlight the features and fixes to be released in this month's patch Tuesday for NBRS-5.0 and NBRS-3.0. We continue to develop, and will continue to support, NBRS-3.0 for the foreseeable future (several years).

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
December 2013

You can contact us here at HQ by eMail (nbhq@network-box.com), or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

twitter http://twitter.com/networkbox
facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse
LinkedIn http://www.linkedin.com/company/network-box-corporation-limited
Google+ https://plus.google.com/u/0/107446804085109324633/posts

IN THIS ISSUE

Network Box 5 SSL Proxy

Network Box 5 includes a SSL Proxy security module that provides for identification, decryption, encryption, certificate validation, and protection of SSL network traffic. This article describes, in detail, how this proxy operates.

Definition

Transport Layer Security (TLS) and its predecessor, **Secure Sockets Layer (SSL)**, are cryptographic protocols which are designed to provide communication security over the Internet. They use X.509 certificates and hence asymmetric cryptography to assure the counterparty whom they are talking with, and to exchange a symmetric key. This session key is then used to encrypt data flowing between the parties. This allows for data/message confidentiality, and message authentication codes for message integrity and as a by-product message authentication. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP). An important property in this context is forward secrecy, so the short term session key cannot be derived from the long term asymmetric secret key.

Wikipedia
http://en.wikipedia.org/wiki/Secure_Sockets_Layer

So, SSL (aka TLS) is a protocol used to protect network traffic. It is commonly used as an option in such protocols as HTTP (HTTPS), SMTP (SMTP), IMAP (IMAPS), etc. The protocol is either used directly over a dedicated port (e.g.; tcp/443 for HTTPS, tcp/993 for IMAPS) or enabled mid-protocol (e.g.; CONNECT for proxied HTTP, STARTTLS for SMTP).

By convention, we refer to SSL/TLS by its original name SSL in the rest of this article (noting that both protocols are covered by the Network Box SSL proxy).

Certificate Exchange

The first stage of SSL consists of certificate exchange using asymmetric cryptography (usually RSA). Typically, a client connects to an SSL enabled server, and sends a message to the server to initiate the SSL communication link. The server responds with it's certificate. This certificate is, at its core, a cryptographically signed object containing the name of the server, the dates the certificate is valid, and other optional information. The certificate is signed by an authority that both the client and server trust. For example, say a client wants to securely connect to WWW.ACME.COM - it first looks up the IP address, makes a tcp/ip connection, then initializes SSL. The server provides its certificate (which contains the name WWW.ACME.COM and is signed by a certificate authority trusted by both the client and the server) and the client validates that certificate. It is this process that provides the core foundational security of the SSL protocol. Once the secure link has been negotiated, the rest is just bulk symmetric encryption and usually very fast and relatively simple.

The vast majority of security problems with SSL come at this certificate exchange stage. Who determines which certificate authorities are trusted? Who says what to do if a server certificate does not validate (for example, it is signed by an untrusted authority, or has expired)? The answer to these questions is usually the end-user, and study after study has shown that end-users will click whatever they need to click to get access to what they want - usually at the expense of security. If an end-user goes to a website, and gets a certificate validation warning, in the vast majority of cases they will just click whatever they need, to get access to the site they want.

The other issue with SSL communications is that they are encrypted, so cannot normally be subject to policy control, anti-malware or other such protection mechanisms.

Man in the Middle

The issue comes if an attacker can position themselves between the client and the server. When the client connects to the server, the attacker then intercepts that connection and provides his own fake certificate to the client. The attacker can then connect to the server as a client themselves. If the client chooses to accept the attacker's certificate (ignoring the trust warnings raised), from then onwards the attacker can decrypt, inspect and modify all the traffic between the client and the server.

Network Box SSL Proxy

The Network Box SSL proxy attempts to solve these issues in three ways:

1. The validation and enforcement of policy regarding SSL certificates is moved from the client to the proxy.
2. Weak SSL options are removed from the SSL negotiation, ensuring that the proxy ➔ server connection is not susceptible to attacks such as BEAST, CRIME, BREACH, RC4, etc.
3. Providing the option to decode SSL traffic for inspection, policy control, anti-malware and other such protection.

The SSL proxy works by intercepting the traffic between clients and servers, in a similar way to a man-in-the-middle attack. Application Identification is used to examine the client traffic, identify the initial SSL negotiation, and mark the connection as SSL protocol. At that point, a policy decision can be made whether to (a) bypass, (b) decode or (c) deny the connection, and this policy decision can be made with a large number of flexible access control rules (such as SSL host being visited, content filtering category, IP addresses, as well as attributes such as HTTP host for the web client protocol). For protocols such as SMTP and HTTP proxies, where the protocol can be promoted to SSL (STARTTLS, CONNECT, etc), this policy decision can be used not just to decode the SSL traffic, but also to enforce the use of standards-comformant SSL protocol in subsequent communications (stopping clients from using CONNECT to indicate an SSL connection, but then passing non-SSL traffic over that connection attempting to bypass policy control).

The SSL proxy contains a SSL Certificate Authority, and to avoid warnings on client workstations, that certificate authority should be installed as trusted on client devices. From that point on, trust enforcement of certificates is moved from the client to the Network Box proxy. Trusted certificates will be re-signed and appear to client browsers as validated and ensured by Network Box directly.

Conclusions

Using the Network Box SSL proxy, administrators can impose effective policy control over the negotiation stage of SSL (which negotiation options are supported, which certificate authorities are trusted, which sites should be bypassed, etc), as well as choose to enforce/bypass SSL decoding using a rich set of access control rules. Decoded traffic is subject to the same policy control and protection (such as anti-malware) as plaintext traffic.

Network Box Five

NBRS-5.0

On Tuesday, 3rd December 2013, Network Box will release our patch Tuesday set of enhancements and fixes.

NBRS-5.0 Features

December 2013

The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for NBRS-5.0, these include:

- Release of security module for SSL VPN
- Release of security module for PPTP VPN
- Release of security module for SSL proxy
- Release of security module for Frontline IPS
- Release of security modules to support NBRS-5.0 NOCs and bi-directional configuration synchronization
- Enhancements for firmware updates, to minimize disruption caused by service restarts
- Enhancements to Administrative Web Portal, to support import and export of reports, and a report template system
- Enhancements to Web Application Firewall and Web Server protection, to support site path routing
- Support for a generic SSL proxy
- Support for SSL proxy of web client traffic (both transparent and directed proxy CONNECT method)
- Enhancements to enable caching of SSL proxy server contexts
- Enhancements to add support for RC4 in SSL client contexts
- Minor enhancements to the Administrative Web Portal
- Enhancements to IPSEC VPN modules (for aggressive mode, PFS and others)
- Enhancements for PNAT support in network and proxy Network Address Translation
- Various other general minor system enhancements and fixes

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local NOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local NOC. They will be arranging deployment and liaison.

Network Box Certified ISO 9001 / ISO 20000 / ISO 27001 Security Operations Centre

NBRS-3.0 Features

December 2013

On Tuesday, 3rd December 2013, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for NBRS-3.0, these include:

- Changes to box model identification for S-25 model
- Extensions to Global Monitoring System for both NBRS-3.0 and NBRS-5.0 support, as well as migration of boxes from NBRS-3.0 to NBRS-5.0
- Revisions to gateway monitor system, to allow for change of routes upon gateway failure
- Various (mostly internal) enhancements to Box Office and support systems

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local NOC will contact you to arrange this if necessary.

Network Box 5

1 November 2013

Network Box launched its new managed security platform, Network Box 5 (NBRS-5.0). The state-of-the-art Network Box 5 software platform, consists of more than one-point-one million lines of code; representing more than one hundred and thirty eight thousand hours of highly dedicated research and development. This has resulted in the new software platform, being up to 8 times faster, than the previous Network Box 3 (NBRS-3.0) software platform.

To compliment the software, Network Box has also launched a new set of 64-bit hardware units. Every model is based on multi-core CPUs, fully supports Hyper-Threading Technology and utilizes high speed DDR3 RAM. The Network Box 5 hardware range, is designed to offer exceptional performance and reliability.

For more details, please visit:
http://www.network-box.com/nbrs5

NOVEMBER 2013 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	419	-5.4
Signatures Released	1,083,112	+75.3
Firewall Blocks (/box)	854,430	+3.9
IDP Blocks (/box)	108,873	+11.7
Spams (/box)	11,506	-16.6
Malware (/box)	5,847	+206.1
URL Blocks (/box)	112,101	-11.3
URL Visits (/box)	3,098,491	+7.2

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box UK
Network Box USA
Contributors

SUBSCRIPTION

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2078
Fax: +852 2736-2778
www.network-box.com