MAY 2015

www.network-box.com

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the May 2015 edition of In the Boxing Ring

This month, we present the second in our two part series on proxying the SSL protocol. For the first part, please refer to the April 2015 edition of the *In the Boxing Ring* newsletter.

Previously, we talked about how Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are cryptographic protocols have been used to secure communications for more than 10 years. We've also presented how they rely on the certificate, how that certificate is verified, and how man-in-the-middle interception can take place. In pages 2-3, we discuss in detail how Network Box supports SSL in it's Network Box 5 product.

On pages 4–5, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. We continue to develop, and will continue to support, Network Box 3 for the foreseeable future (several years).

Finally, it has been a busy month for Network Box. Not only did Network Box win a PC3 Platinum Brand Award in the *Managed Security Services* and *Unified Threat Management* categories; Network Box 5 won multiple awards at the Silicon Valley Communications *Info Security Awards 2015*, and a *Most Valuable Product 2015 Award* from Computer Technology Review USA.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
May 2015

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

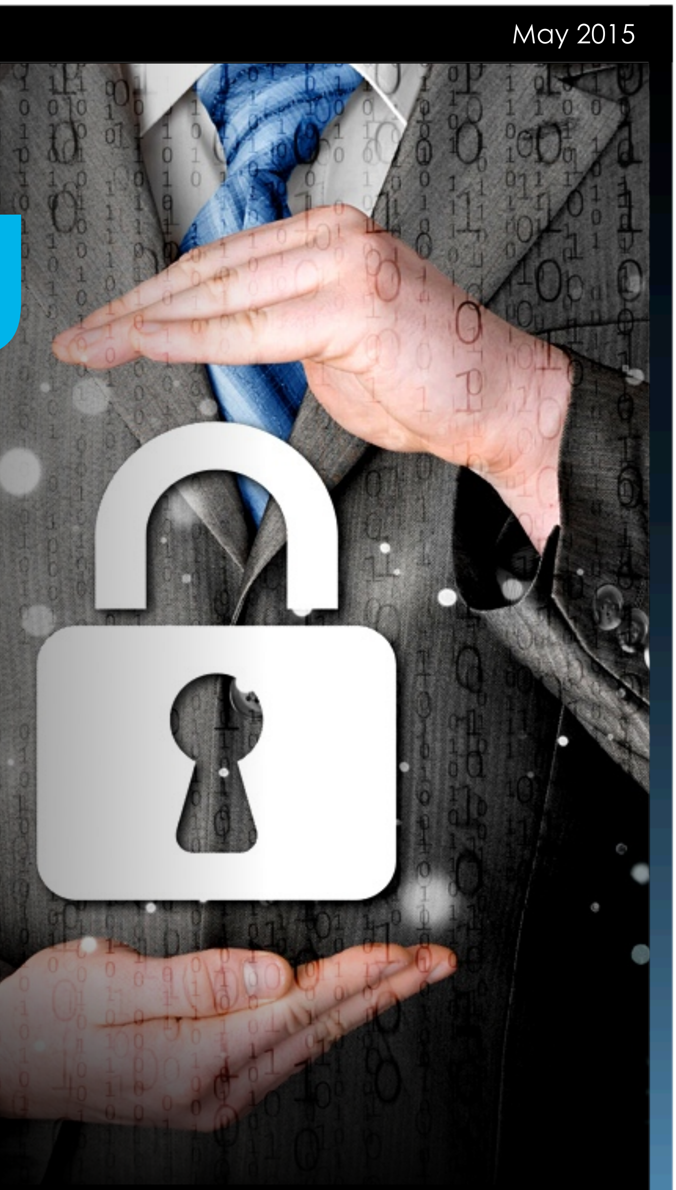
facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

- **Silicon Valley Communications** Info Security Awards 2015 Grand Trophy
- **Computer Technology Review USA** Most Valuable Product
- **PC3 Platinum Brand Awards 2015**
  – Managed Security Services
  – Unified Threat Management



Proxying SSL

part (2 of 2)

We've already talked about how Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are cryptographic protocols have been used to secure communications for more than 10 years. We've also presented how they rely on the certificate, how that certificate is verified, and how man-in-the-middle interception can take place. Now, let's discuss how Network Box supports SSL in it's Network Box 5 product.

SSL as a Filter

The first key concept is that in Network Box 5, TLS/SSL is treated as an encapsulation layer. HTTPS is purely the HTTP protocol encapsulated in an SSL stream. Similarly SMTPS is SMTP in SSL, POP3S is POP3 in SSL, and IMAP4S is IMAP in SSL. In general, any arbitrary data stream or protocol can be encapsulated in SSL for protection.

Network Box 5 treats SSL interception as a filter on the communication channels. The device can be configured to add or remove SSL from either the input or output sides of a communication. If SSL is chosen to be removed, then the resulting plain text can be analyzed further.

The SSL negotiation is always initiated from the client side, and can be started in one of two ways:

1. Fixed Port (for example tcp/443 for HTTPS). The client starts the negotiation of SSL immediately after the network connection has been established.

2. Command based (for example CONNECT for http proxy, STARTTLS for SMTP, etc). The client first initiates a switch to SSL, using a protocol-level command such as CONNECT or STARTTLS. Then, once the server acknowledges that, both clients assume the connection is now ready for SSL and the client starts the negotiation of SSL.

For either type, SSL identification and decoding starts with the client-initiated SSL negotiation.

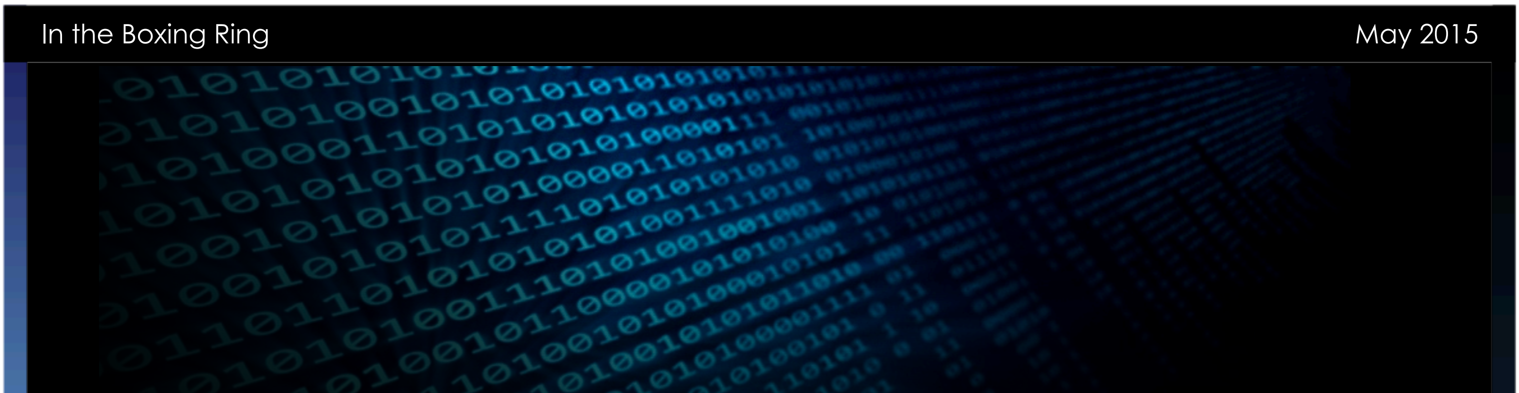
Client Side vs Server Side

Typically, there are two scenarios where Network Box SSL proxying can be involved:

1. Client Side. Here, clients (typically in the LAN/DMZ) are connecting out to external public SSL servers. In this case, the certificate for the SSL server is not under the control of the Network Box admin. SSL Man In The Middle style interception and proxying must be used to decrypt the traffic.

2. Server Side. Here, clients (typically on the Internet) are connecting in to internal SSL servers (typically in the DMZ). In this case, the certificate for the SSL server is under control of the Network Box admin, but the client policies are not. The server certificate and private key would typically be installed on the Network Box, so that the Network Box SSL proxy can use those to act on behalf of the server and decrypt the incoming SSL sessions.

As you can see, the technologies used for both are very different, so let's discuss them further individually.



Client Side SSL
Man in the Middle Proxying

The Network Box 5 SSL Man In the Middle proxy works by intercepting SSL communications between the client and the server. Two separate SSL sessions are maintained - one between the client and the proxy, and the other between the proxy and the server. For more information on the technical aspects of this, please refer to the part 1 article in the April 2015 In The Boxing Ring newsletter.

There are various policy rule points in the Network Box proxy, including:

- The decision on whether to decode the SSL traffic is made shortly after connection time, once the client SSL negotiation message has been received. The options available are (a) bypass the traffic without decode, (b) permit the traffic and decode it, or (c) deny the connection.
- Once the server certificate has been received, it is validated. Checks are made for items such as certificate signing chain, as well as issue and expiry dates. The result of those checks is then available as a policy decision to (a) permit it anyway, or (b) deny the connection.
- When inspecting a communication channel for SSL traffic, at some point a decision is made whether there is actually an SSL negotiation being attempted. In the case where the traffic is not SSL, a policy decision is made whether to (a) bypass the traffic and allow it, or (b) deny the connection. An example here is the HTTP proxy CONNECT statement. That should be used to switch to SSL, and a policy decision can be made if the client does not actually negotiate SSL after the CONNECT statement (as they are most likely trying to bypass firewall policy).

Server Side SSL Fronting

Network Box 5 can be used to ‘front’ SSL communications at the gateway. Rather than deploying a SSL enabled server, instead the SSL certificate and private key can be installed on the Network Box, and the SSL connection terminated there. With this arrangement, the connection from client to proxy is SSL protected. The connection from proxy to server can either be plaintext, or re-encoded as SSL again.

The advantage of SSL fronting is that it allows protection technologies such as WAF and anti-ddos to be deployed even for SSL protected services.

Why Decode SSL?

So, given the above technologies and capabilities, we come to the core question of why would we want to decode SSL?

The simple answer is that we want to enforce policy control and have the capability to apply protection technologies for traffic protected by SSL, in the same way we do for plaintext traffic. As more and more of the Internet’s communications move to SSL, less and less is subject to policy control and protection, unless we deploy SSL decoding capabilities. An example is google safe search. Sure, we can enforce safe search at the proxy, and it works well in school and home environments. But, google search has now moved to SSL, and without SSL decoding, safe search cannot be enforced at the proxy.

Another reason is that the SSL certificate verification process occurs largely at the client workstation, with the end-user being responsible for the decision as to whether to accept/reject a problem with a particular connection. End-users are typically not trained in the security implications of such decisions, and in general it is better to leave such security policies up to the administrator, to be enforced at the gateway.

Protocol Promotion

One unique feature of the Network Box 5 SSL proxy, that comes from our implementation as a filter, is that the SSL decode mechanism can be combined with other functions such as application identification. We can intercept network communications generically, use the SSL filter to decode the SSL stream, and then apply application identification to that decoded stream. With such a capability, we can detect the full suite of 1,000+ applications, even if they are encrypted in SSL.

Moreover, once we’ve used the filter to decode SSL, and identified an application such as SMTP, HTTP, POP3, etc, we can ‘promote' the stream to a protocol specific module for further protection. An example of this would be to intercept all outbound TCP traffic, filter out SSL if detected, then if the application type is detected to be HTTP (originally HTTPS when protected by SSL), transparently switch the traffic through to the webclient module for url policy enforcement, anti-malware scanning, and safe search enforcement.

We hope that you now have an understanding of the SSL/TLS protocol, and how Network Box 5 can filter it out of your network communications, to allow you to apply policy control and other protection technologies to the underlying data stream.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 5th May 2015, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days.

Network Box 5 Features

May 2015

This month, for Network Box 5, these include:

- Support for new VPN-5 Network Box model
- Enhance filter control for configuration change history reports
- Performance and stability improvements related to reporting on holistic transactional records
- Support for holistic vpn event records
- Support for ports other than tcp/25 with the mail server security module and transparent smtp scanning
- Support for a new administrative console attack status overview report
- Improvements to logging of smtp server connections, with mix of good and bad (rejected) recipients
- Enhanced configuration selection of specific authentication helpers to use for a particular purpose
- Support for SSL proxy re-signing of server certificates without keyEncipherment
- Performance and stability improvements to admin web portal live updates
- Improvements to batch resumption in signature push/receive
- Enhanced support for logging of VPN sessions
- Support for multiple eMail attributes in envelope verification over LDAP
- Support for internationally encoded filenames in mail scanning policy enforcement
- Automatic detection of Microsoft Office documents containing macros, for policy enforcement
- Performance and compatibility improvements with directed web client proxy related to authentication caching
- Enhanced UTF-8 support in password store
- Performance improvements in authentication helpers, for sites with thousands of user entities
- Performance improvement in admin web portal widgets using ‘recent’ range
- Enhanced support for learning of IPv4 and IPv6 address attributes in the entity system
- Performance improvements in KPI reporting
- Enhanced support in proxy web server (and WAF) for authentication at the gateway
- Improvements to logging of PPTP VPN connections
- Improvements to logging of SSL VPN connections
- Introduce support for basic Radius authentication against an external Radius server
- Improvements to compatibility with IE11 and user/admin web portals

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 SOC will contact you to arrange this if necessary.

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

Network Box 3 Features

May 2015

On Tuesday, 5th May 2015, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for Network Box 3, these include:

- Enhancements to Box Office related to device provisioning and optional services
- Improvements to scan correlation and reporting regarding selective bypass of defined event types
- Various (mostly internal) enhancements to several internal 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 SOC will contact you to arrange this if necessary.

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 2736-2083
Fax: +852 2736-2778

www.network-box.com

Silicon Valley Communications

Info Security Grand Award 2015

▲ *Network Box USA Chief Technology Officer, Pierluigi Stella, accepted the Grand Trophy on behalf of Network Box*

Network Box has been awarded the Silicon Valley Communications 11th Annual 2015 Info Security Products Guide **Grand Trophy**, a recognition that is among the most coveted within the information security industry. The Trophy was presented during the Info Security Products Guide Awards Dinner held in San Francisco on April 20th, 2015.

Network Box also walked away with **Three Gold** Global Excellence Awards, for *Network Box 5*, in the categories of *Security Products and Solutions for Small Businesses and SOHO*; *Education*; and *Retail*.

LINK: http://www.infosecurityproductsguide.com/world/

Computer Technology Review USA

Most Valuable Product 2015

Network Box 5 won a highly prestigious **Most Valuable Product 2015 Award** from Computer Technology Review USA.

LINK: http://wwpi.com/network-box-5/

PC3 Platinum Brand Awards 2015

Network Box we won a PC3 Platinum Brand Award 2015, at the 10th Annual PC3 Awards, in both the *Managed Security Services*, and the *Unified Threat Management* categories. The awards ceremony took place on the 24th of April 2015.