NETWORK BOX
NEXT
GENERATION
MANAGED SECURITY

network-box.com

In the Boxing Ring DECEMBER 2021

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the December 2021 edition of In the **Boxing Ring**

Season's Greetings. This month, we are talking about **Network Box Web Client Protection**. Network Box offers an optional Web Client Proxy, providing secure management of web client traffic, using standards-compliant proxy technology. On pages 2 to 3, we discuss the Network Box Web Client Proxy, including its functionality and optional configurations.

Also this month, Network Box Germany was at bIT21. During the event, Network Box gave a talk title, "This is how the Medical Industry meets the IT security guidelines." And in this month's Global Security Headlines, the biomanufacturing sector was affected by the Tardigrade Malware; and security issues were encountered by Palo Alto, GoDaddy, Sky UK, Robinhood, and the FBI.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
December 2021

Stay Connected

You can contact us here at Network Box 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:

https://twitter.com/networkbox

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

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

https://www.youtube.com/user/NetworkBox

In this month's issue:

Network Box Web Client Protection

Network Box offers an optional Web Client Proxy, providing secure management of web client traffic, using standards-compliant proxy technology. This article describes the Network Box Web Client Proxy, including its functionality and optional configurations.

The proxy increases security and control by isolating web clients from the Internet. In addition, the following functionality is available:

- Support for 'transparent' and 'directed' proxy modes
- Authentication of client access to the web via various mechanisms, including Windows NT LAN Manager (NTLM) and basic authentication, kiosk mode, and entity IP address tracking
- Logging and statistical traffic analysis
- URL Categorization and Content Filtering Policy enforcement
- Anti-Malware scanning of HTTP traffic
- Policy control of web access via access-control rules
- Policy control of other traffic using HTTP and HTTPS protocols
- Support for SSL scanning and policy enforcement

Isolation of Web Clients from the Internet

The Network Box Web Client Proxy can operate in either of the standard modes or both simultaneously:

1. Directed Proxy Mode

The Directed Proxy Mode is used when a web client is aware of and is directed to use a specified proxy. In this mode, the web client is configured not to contact websites directly via the normal name->address DNS lookup, but to direct all web access to a specified host and port (the specified web proxy). The advantage of this mode is that it supports client HTTP proxy authentication directly and also supports the HTTP proxy CONNECT method for control of protocols tunneling over the HTTP proxy. For larger deployments, Web Proxy Auto-Discovery (WPAD) and Dynamic Host Configuration Protocol (DHCP) options can be used to auto-configure the clients.

2. Transparent Proxy Mode

The Transparent Proxy Mode does not require any web client reconfiguration. In this mode, the web client performs a normal name->address DNS lookup and then attempts to contact the remote web server directly. Network Box transparently intercepts the outbound connection (usually via interception of a defined port such as TCP/80), and directs it into the web client proxy. The advantage of this mode is that it requires zero web client configuration.

Authentication of Client Access to the Web

It is beneficial to authenticate the web client user before access is granted in some configurations. For example, where multiple users use one individual workstation, or to be able to log access by username (rather than just IP address) and to be able to implement per-user policy controls (as opposed to per-IP).

Network Box supports various mechanisms for this:

1. Basic Authentication

The Basic Authentication system is supported by the 'directed' proxy protocol. In this mode, the web client proxy informs the web client that authentication is required and refuses web access without such authentication. The web client then prompts the user to enter his username + password, and the web client passes the username + password in each future web request. Network Box Web Client Proxy, using helper modules, performs the actual validation of the username and password.

2. NTLM Authentication

The NTLM Authentication system is supported by the 'directed' proxy protocol. In this mode, the web client proxy cooperates in a three-way challenge-response handshake between the client, the proxy, and a Microsoft domain server. The advantages of this system are that it is secure (the password is never known to the proxy, but the proxy is assured it has been authenticated by the domain server), the exchange of authentication credentials is securely managed, and no login box is presented to the user as the credentials are picked up automatically from the existing domain login.

3. Kiosk Mode Authentication

Kiosk Mode works by presenting the user, on first connection, with a web page requesting authentication by username and password. Network Box Web Client Proxy, using helper modules, performs the actual validation of the username and password. In general, this authentication remains valid until the web client is idle for a pre-configured time period, but the option also exists to request re-authentication periodically.

4. IP address Entity Allocation

The Network Box Web Client Proxy can use IP address entity attributes to automatically associate traffic to/from that IP address with the specified entity user. Gaining all the advantages while completely avoiding the requirement to authenticate.

IP address Learning from Active Directory Logins

As an alternative to manual administrative maintenance of entity IP address attributes, a small log forwarding agent can be installed on Microsoft Active Directory servers so that user login/logout events can be forwarded to the Network Box system to maintain the IP address attributes automatically. The approach used is that once a user logs in using Active Directory, the IP address the user is logging in from is associated with the user's entity (and removed from any other entities it was previously associated with). Traffic to/from that IP address can be associated with that entity user from then onwards.

Logging and Statistical Traffic Analysis

As web requests and content pass through the Network Box Web Client Proxy, the transactional details are logged and stored. In addition, statistical summaries are automatically maintained to generate efficient statistical traffic reports. The Admin Portal administrative web interface provides access to status and analysis reporting on this information.

The status information provided includes monitoring activity in real-time, as well as transaction-level searches and filters to research and monitor the activity of a particular website, IP, or user.

The analysis system provides historical reporting, by month / day / hour / minute, and by User / IP / Category / Site. The reporting is primarily geared towards policy enforcement results and bandwidth summaries.

Additionally, a periodic report can be configured to email a summary report of key web client metrics using PDF document format.

SSL Support

The Network Box Web Client Proxy includes full support for SSL interception, scanning, and policy control in 'transparent' and 'directed' (via CONNECT method) modes. As more and more of the web is encrypted, this is becoming more important nowadays than ever before.

However, Network Box goes beyond basic SSL scanning to full SSL policy control. We provide administrative control over the entire SSL policy, including policies for certificate validation, trusted CAs, expiration control, minimum protocol level enforcement, etc.

Even without full SSL decryption enabled, Network Box can still look at the Server Name Indication (SNI) field during SSL negotiation (which contains the name of the remote SSL server being connected to), and use that for categorization and policy control.

URL Categorization, Content Filtering, Anti-Malware, and Policy Enforcement

The Network Box Web Client Proxy is a categorization engine at its core. It examines traffic passing through, classifies and categorizes it, and then applies policy rules to determine whether to permit or deny it (as well as log the activity appropriately).

As part of this classification and categorization system, a massive signature database is used to categorize URLs into a set of 60 categories covering both productivity as well as core (usually restricted) categories. These categorizations are fully customizable by the administrators and Security Operations Centres.

The Network Box Web Client Proxy supports scanning of traffic for viruses, worms, spyware, adware, and other malware. Anti-malware engines are used to scan both the web request (identifying both malicious requests and uploading of malicious attachments) and response and classify the traffic as malicious if appropriate.

These categorizations, classifications, and other metadata (such as IP addresses, entity user, application identification, server name, protocol, method, etc.) can then be used in policy control rules.

> **The Network Box Web Client Proxy provides an extremely flexible and highly configurable system for enforcing a defined policy on web client traffic. Full management reporting and configuration control are provided as part of the system.**

Network Box HIGHLIGHTS

NETWORK BOX

Network Box Germany
bIT21

Network Box Germany was at bIT21, which took place in Dortmund, Germany. During the event, Network Box gave a talk title, "This is how the Medical Industry meets the IT security guidelines."

Newsletter Staff	Subscription
Mark Webb-Johnson Editor	Network Box Corporation nbhq@network-box.com or via mail at:
Michael Gazeley **Kevin Hla** Production Support	**Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong
Network Box HQ **Network Box USA** Contributors	Tel: +852 2736-2083 Fax: +852 2736-2778 www.network-box.com

Copyright © 2021 Network Box Corporation Ltd.

Global Security Headlines

The Street
7 Million Robinhood Users' Data Exposed As Stock Falls After Hours
LINK: https://bit.ly/3ojsGq1

Reuters
Hackers compromise FBI email system, send thousands of messages
LINK: https://reut.rs/3EzLxTL

Threat Post
Massive Zero-Day Hole Found in Palo Alto Security Appliances
LINK: https://bit.ly/31oduiP

Threat Post
6 Million Sky Routers Left Exposed to Attack for Nearly 1.5 Years
LINK: https://bit.ly/3phgSUs

SC Magazine
Over 1 million GoDaddy WordPress accounts breached
LINK: https://bit.ly/3ddqWIC

SC Magazine
HHS: APT targeting biomanufacturing with stealthy Tardigrade malware
LINK: https://bit.ly/3ddQ8Pl