Carbon Black Server Configuration: Using a Reverse Proxy

Contents

Carbon Black Version 5.1.0
Document Version 5.1.0.a

25 September 2015

Bit9, Inc.
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@bit9.com
Web: http://www.bit9.com

Copyright © 2004-2015 Bit9, Inc. All rights reserved. This product may be covered under one or more patents pending. Bit9 and Carbon Black are trademarks of Bit9, Inc. in the United States and other countries. Any other trademarks and product names used herein may be the trademarks of their respective owners.

Overview

Communication between the Carbon Black Enterprise Server and its sensors is handled via HTTPS and validated using both server-side SSL certificates and sensor-side client certificates. If you want to use a Reverse Proxy in your Carbon Black environment, special steps must be taken to allow validation of communications with the proxy if SSL termination will be performed. This document provides the configuration necessary to set up the Carbon Black Server for use with a Reverse Proxy. Both standalone servers and clustered Carbon Black Servers can be configured to use a Reverse Proxy. If SSL termination is not being performed on the Reverse Proxy, no additional steps will be required for proper communications.

When a sensor communicates with a Carbon Black Server, two forms of "authentication" or "verification" occur. The sensor receives the Carbon Black Server's SSL server certificate and validates it against its local copy to verify the server's identity. The sensor will then provide the Carbon Black Server its client certificate so that the Carbon Black Server can verify the sensor's identity.

To allow validation of sensors in the Reverse Proxy environment, the proxy must send the Carbon Black Server an HTTP header containing the Serial Number of the client certificate. The Carbon Black Server then verifies the Certificate ID against its internal database to complete all sensor communications.

A client certificate is not used for validation of communications between the Reverse Proxy itself and the Carbon Black Server. Instead, the identity of the Reverse Proxy is specified in the Carbon Black Server configuration file (cb.conf).

Note: Most of the complexity in configuration of a Reverse Proxy is in the proxy itself; this document does not describe steps involving specific Reverse Proxy tools or their configuration.

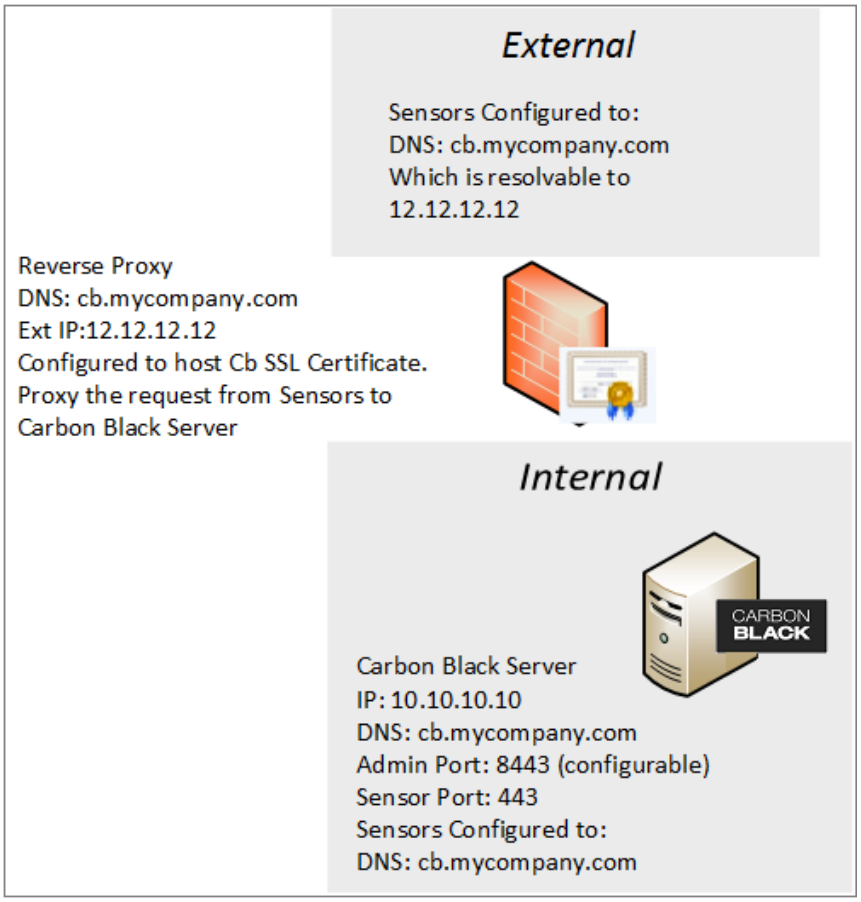
Limitations

- Currently the Carbon Black Server supports use of a single Reverse Proxy IP address only in cb.conf.
- The cb.conf configuration below must use the proxy IP address; use of a DNS name is not supported.

Example Proxy Configuration

Before beginning the configuration tasks, determine whether all of your sensors will be directed to the proxy or whether you will instead have a hybrid environment in which some sensors communicate to the proxy and some directly to the Carbon Black Server. Depending on the complexity of DNS configuration to be used there may be other options available besides the example listed below. In the example below, the internal and external DNS names used for sensor communication are the same, so there is an expectation of split DNS.

Note: Configuration of a Reverse Proxy in a clustered environment can be complex. If you have a clustered environment and do not follow this example of a split DNS with each node in a cluster having a separate DNS/IP combination, consult Bit9 + Carbon Black Professional Services for assistance.



Configuring the Reverse Proxy

Two Carbon Black-specific configuration tasks must be performed on the Reverse Proxy:

- Copy the appropriate certificates from the Carbon Black Server to the Reverse Proxy.
- Modify message headers on the Reverse Proxy so that they include information required by the Carbon Black Server to validate and identify sensors. Some of the headers are mandatory and some are optional.

Copying Certificates from the CB Server

The Reverse Proxy will need to validate the client certificates presented by Carbon Black sensors, and the proxy must provide the server certificate for validation by the sensors. This involves copying the certificate files from the Carbon Black Server to the Reverse Proxy. Note that in a clustered environment, all nodes use the same client and certificate files, so you can copy the just files from the Master node in that case. The files to copy are:

- `/etc/cb/certs/cb-server.crt` (server SSL certificate)
- `/etc/cb/certs/cb-server.key` (server SSL certificate key)
- `/etc/cb/certs/cb-client-ca.crt` (SSL client certificate for server to validate sensors)

Headers Expected by the Carbon Black Server

The following headers for the connection with the Carbon Black Server either must or can be modified or added by the Reverse Proxy:

- X-Client-Cert-ID (required)
- X-Real-IP (recommended)
- X-Forwarded-For (optional)

X-Client-Cert-ID

This header is **required** to be set to the Serial Number of the client certificate presented in the client certificate used by the sensor. If this is not set to the correct Certificate Serial Number then the Carbon Black Server will reject the connection.

The X-Client-Cert-ID header must be in one of the following formats:

- d4e177cd28814d7084fff10f72e8828a
- d4:e1:77:cd:28:81:4d:70:84:ff:f1:0f:72:e8:82:8a

X-Real-IP

This header should contain the real IP address of the sensor connecting through the proxy. Inclusion of this header is highly recommended. It allows additional logging on the Carbon Black Server to represent the real IP addresses of the reporting sensors.

X-Forwarded-For

This header contains a list of all proxies/forwarding servers within the sensor-to-server communication. This is an optional header. If set correctly on all proxies, it will contain a list of all proxies the connection traversed at the Carbon Black Server.

Configuring Carbon Black Servers for Reverse Proxy

On the Carbon Black Server, setting up a Reverse Proxy involves modification of the cb.conf file, restarting the server(s), and validation that the sensors and server(s) are able to communicate via the proxy. The first step must be performed on all servers in a clustered environment.

To configure Carbon Black Server(s) to use a Reverse Proxy for sensor communications:

1. On the standalone or master server, edit the **/etc/cb/cb.conf** file, search for and uncomment the line **ReverseProxyIP**, and provide the IP address of the proxy server as the value for that line, using the format shown in the example below. Save the file.

   ```
   # Reverse Proxy Server Setting. If this is set Nginx will not check client
   # Certificates from the reverse proxy. For Sensors reporting through the
   # Reverse Proxy, the proxy needs to be configured with the client certificate
   # and private key from the CB server for the sensors. Also the X-Client-Cert-Id
   # header Must be set by the Reverse Proxy to the ID of the client certificate
   # used by the Sensor. It is also recommended to set the X-Real-IP header to
   # the correct address on the reverse Proxy.
   # Details for the configuration and requirements for a Reverse Proxy are
   # Available from Support.
   # Note the IPv4 address of a reverse proxy is in IPv6 wrapped format.

   ReverseProxyIP="::ffff:192.168.1.10"
   ```

   Note: The separate document *Carbon Black Server Configuration File (cb.conf)* for version 5.1 provides for general information about editing this file. It is available on the Bit9 + Carbon Black Customer Portal.

2. If you are setting up a Reverse Proxy in a clustered environment, repeat step 1 on each minion server.

3. Restart the cb-enterprise service on a standalone server, or restart the cluster:

   For a standalone server:

   ```
   service cb-enterprise restart
   ```

   For a cluster:

   ```
   /usr/share/cb/cbcluster stop

   /usr/share/cb/cbcluster start
   ```

4. In the Carbon Black console interface, validate that the Sensor Group and Server Node URLs match what is to be expected in terms of DNS for sensor communications. The Server URL for a Sensor Group appears on the Edit Group Settings dialog accessible via the **Administration > Sensors** page. The node URL is located on the **Administration->Settings->Server Nodes** page. Each server URL will need to be properly resolved in order for each sensor to communicate with the Carbon Black Server, whether it is using direct communication to the server or using the Reverse Proxy.
   See the *Carbon Black User Guide* for more information about Sensor Groups and Server Settings.

Contacting Carbon Black Support

For your convenience, Bit9 + Carbon Black Technical Support offers several means of contact:

Technical Support Contact Options
Web: www.bit9.com
E-mail: support@bit9.com
Phone: 877.248.9098 (877.**BIT9**.098)
Fax: 617.393.7499
Hours: 8 a.m. to 8 p.m. EST

When you call or e-mail Bit9 + Carbon Black technical support, please provide the following information to the support representative:

Required Information	Description
Contact	Your name, company name, telephone number, and e-mail address
Product version	Product name (Bit9 Server, Bit9 Agent, or Bit9 Software Reputation Service) and version number
Hardware configuration	Hardware configuration of the Bit9 Server or computer (processor, memory, and RAM)
Document version	For documentation issues, specify the version of the manual you are using. The date and version of the document appear after the copyright section of each manual.
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, serious, minor, or enhancement