Bit9 + CARBON BLACK	Carbon Black Web Proxy Configuration 16-Oct-2014 Support@Bit9.com

Introduction

The purpose of this document is to describe how to configure Carbon Black (Cb) to utilize a web proxy to communicate with Cb Alliance and Yum Repositories.

Some security policies do not allow direct communication to external web services, but rather require a web proxy to filter traffic (Figure 1). When this policy is enforce, Cb can be configured to utilize the web proxy to communicate with the Cb Alliance server and Yum Repository servers. Follow the steps below to configure the Cb Server to utilize a web proxy server.

NOTE: Cb does not currently support the use of a SSL MITM server. Contact Cb Support for further details

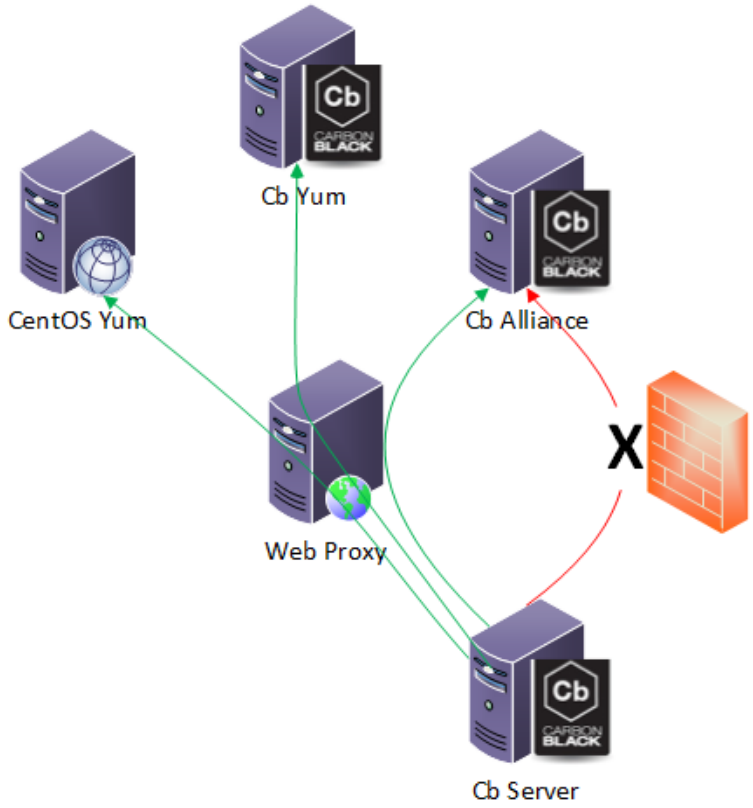

Figure 1 Web Proxy Communication

Table of Contents

Sections

Carbon Black Alliance Proxy Configuration

Note: If the Carbon Black is deployed in a cluster configuration these steps will need to be completed on each server locally. Complete step one on each server before proceeding.

1. Edit the /etc/cb/cb.conf file and modify the following values:
    a. Specify the proxy server to be used for Cb Alliance access
        i. Uncomment the line by removing the “#”
        ii. Replace 127.0.0.1 with Proxy IP or DNS Name
        iii. Replace 3128 with the appropriate listening port of the Proxy Server

```
AllianceClientProxyUrl=http://127.0.0.1:3128
```

    b. Configure the following settings if the Proxy Server is using authentication
        i. Specify the type of authentication. Supported methods are “ntlm” or “basic”.
            1. Uncomment the line by removing the “#”
            2. Identify the type of authentication.

```
AllianceClientProxyAuth=basic
```

        ii. Add the username
            1. Uncomment the line by removing the “#”
            2. Add the username
                a. The username does support “domain\username” format

```
AllianceClientProxyUsername=johndoe
```

        iii. Add the password
            1. Cb can store the password in plaintext or encrypted
            2. To utilize plaintext
                a. Uncomment the line by removing the “#”
                b. Enter the password

```
AllianceClientProxyPlaintextPassword=Password1234
```

3. To utilize an encrypted password
    a. Uncomment the line by removing the "#"
    b. Enter the encrypted password (See Generating an Encrypted Password below)

```
AllianceClientProxyEncryptedPassword=9lWRXW2c3KW61ydeFMl47GF0l1aAoWUGEKGFgIai3ENdpPCo2DKCmUUMEbmvs/Pg
```

    c. Save the file and quit
2. Restart cb-enterprise
    a. Clustered environment (on master run):
    `/usr/share/cb/cbcluster stop`
    `/usr/share/cb/cbcluster start`
    b. Non Clustered:
    `service cb-enterprise restart`

Yum Repository Proxy Configuration

All Carbon Black updates are distributed via the Carbon Black Yum Repository with prerequisites located in the base CENTOS Yum Repository. Since the prerequisites are not located on the Carbon Black yum Server the local Carbon Black server utilizes the default CENTOS Yum repositories to download the packages.

1. Edit the /etc/yum.conf file and add the following values:
    a. Specify the proxy server to be used for Yum Repository access
        i. Add the following line to the file
        ii. Replace 127.0.0.1 with Proxy IP or DNS Name
        iii. Replace 3128 with the appropriate listening port of the Proxy Server

```
proxy=http://127.0.0.1:3128
```

    b. Configure the following settings if the Proxy Server is using authentication
        i. Add the following lines to the file
        ii. Add the username and password
            1. The username does support "domain\username" format

```
proxy_username=johndoe
proxy_password=Password1234
```

    c. Save the file and quit

Generating an Encrypted Password

To prevent a password being stored in Plaintext with in the cb.conf file when using a proxy for alliance communication, a password encryption utility is included within Cb. To produce an encrypted password perform the following steps.

1. Execute script
    a. Ensure to replace “Password1234” with desired the password

    [root@Cb ~]# /usr/share/cb/cbpasswd --encryptpasswd=Password1234

2. Copy the 64, or greater, character encrypted password, like below, for use

9lWRXW2c3KW61ydeFMl47GF0l1aAoWUGEKGFgIai3ENdpPCo2DKCmUUMEbmvs/Pg