Bit9 + CARBON BLACK ARM YOUR ENDPOINTS.	External Carbon Black Sensors Connectivity Options 9-Aug-2014 cb-support@Bit9.com

Introduction

The purpose of this document is to describe the different options for deploying Carbon Black to support external sensors. Carbon Black is built on top of a Linux OS, so any DMZ configuration that Linux supports, Carbon Black can be configured as such. The special requirements that Carbon Black has is the Head-End node must be able to communicate with each Cluster node. From a Sensor perspective, the sensor must be able to check in with the Head-End and push data to its respective Minion, so all nodes in a Carbon Black cluster must have IP/DNS access from the sensor.

Open Firewall to internal Cb Server

Keep the Cb server internal and change the Admin UI port and restrict via iptables. Then configure a Firewall with or without NAT to direct external users via split DNS to the Firewall when external and Cb Server when internal. Example below utilizes NAT.

Requirements

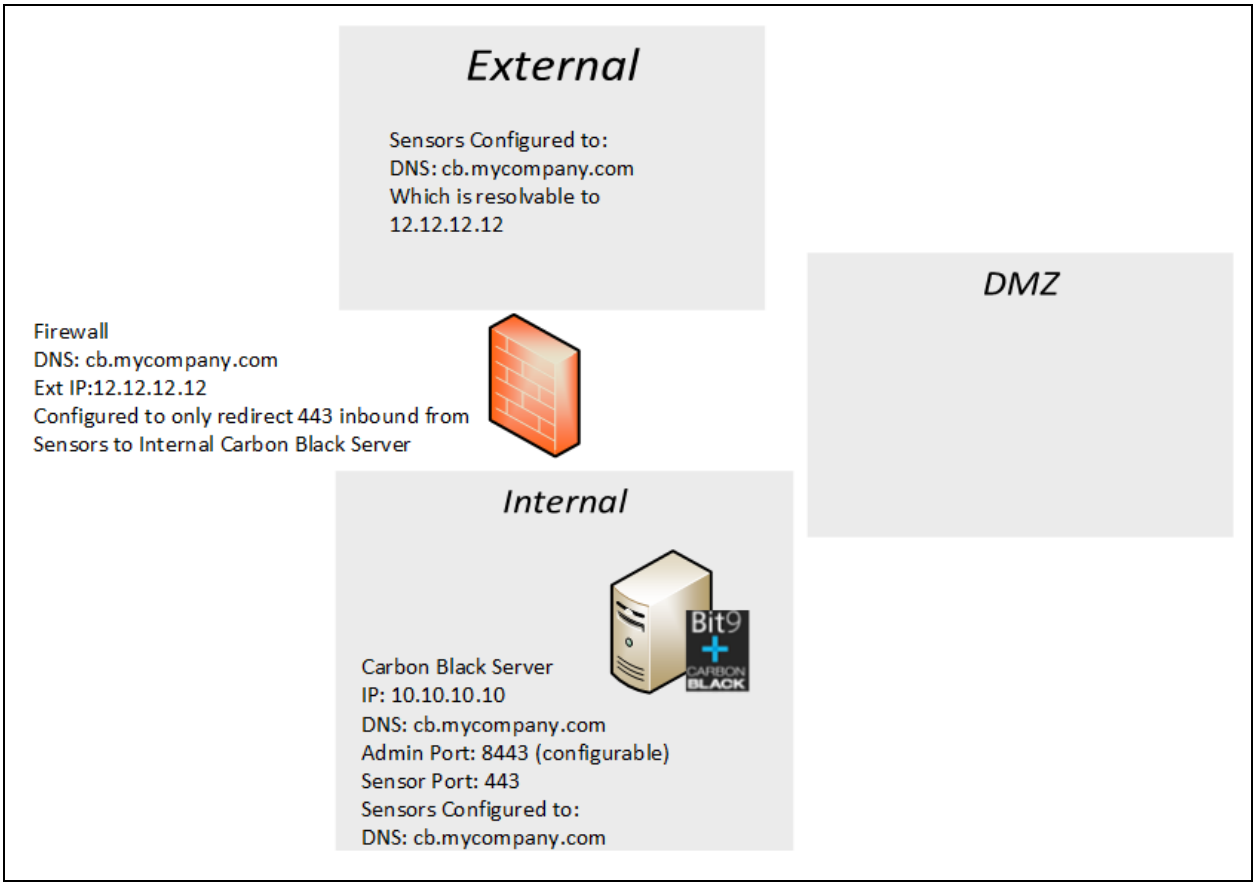
- Layer 3 Firewall, but recommend Layer 7
- Internal DNS Server
- External DNS Server
- External and Internal IP Space

Advantages

- No additional hardware

Limiting Factors

- Internal Cb Server open externally on SSL for ONLY Sensor traffic



Additional Cb Server for DMZ

Place a standalone Cb server in the DMZ, and change the Admin UI port and restrict via iptables. In this configuration the DMZ server would be completely separate from the internal Cb server as we currently do not support a parent/child or forwarding configuration.

Requirements

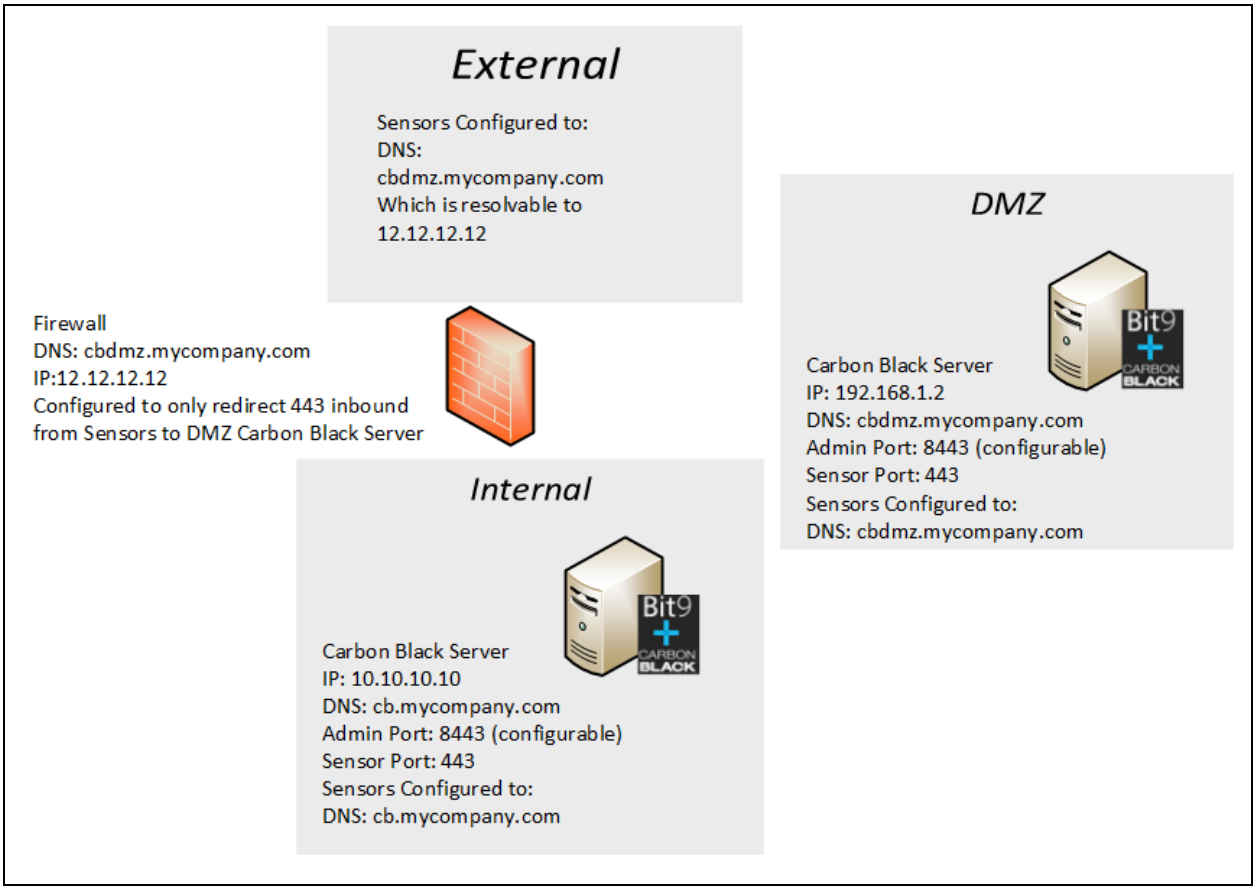
- Layer 3 Firewall, but recommend Layer 7
- DMZ and Internal IP Space
- Additional Cb Server
- Logical Separation for Sensor Distribution to assign Sensors to DMZ Server

Advantages

- Segmentation of data
- Only DMZ Cb Server open externally on SSL for Sensor traffic

Limiting Factors

- Multiple Servers to manage and search (federated search on roadmap)



Place Cb Server in DMZ

Move the existing internal Cb server to the DMZ and change the Admin UI port and restrict via iptables. Then configure a Firewall with or without NAT to direct external/internal users to the DMZ Cb Server. Example below utilizes NAT.

Requirements

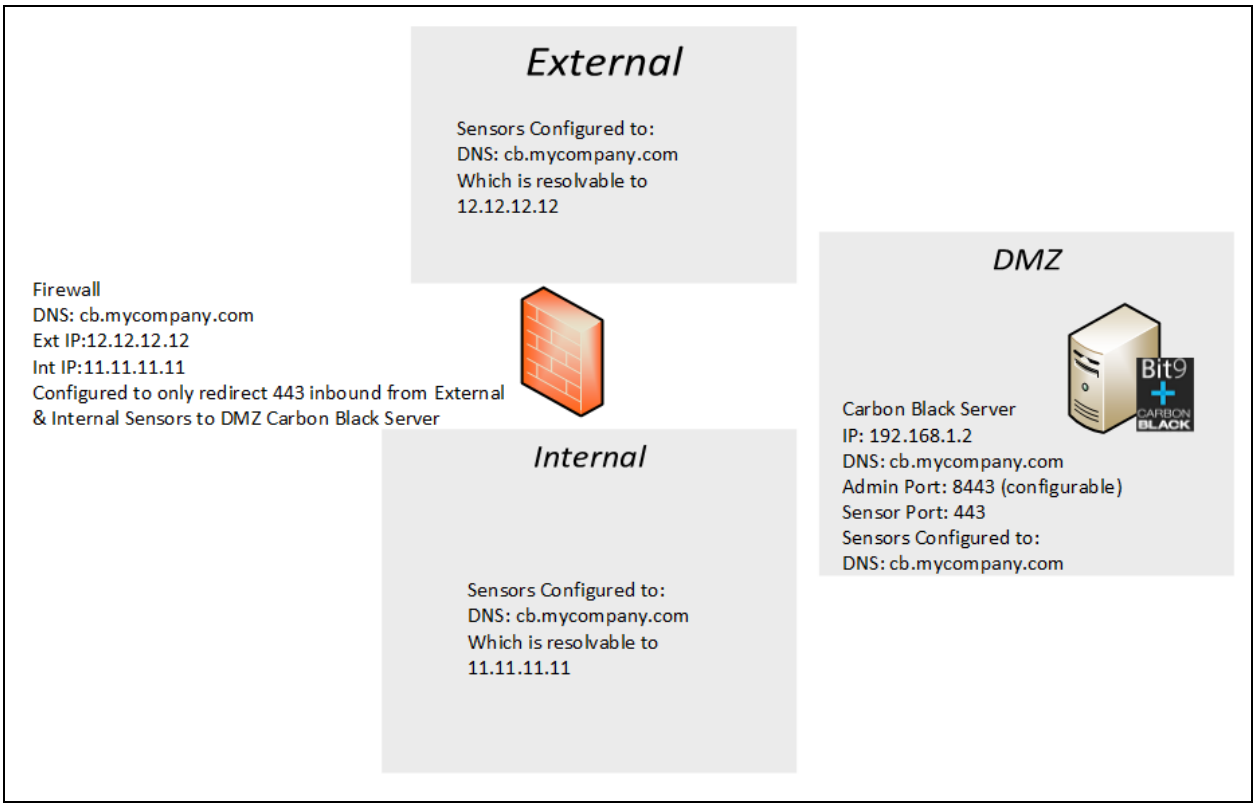
- Layer 3 Firewall, but recommend Layer 7
- Internal DNS Server
- External DNS Server
- External and Internal IP Space

Advantages

- No additional hardware

Limiting Factors

- Increases attack surface as all sensor data is in DMZ



Utilize Reverse Proxy for Internal Cb Server

Keep the Cb server internal, change the Admin UI port, and restrict via iptables. Then import the Cb SSL Server Certificate to a Proxy (F5, Palo Alto, Checkpoint, or similar device) and direct external users via split DNS to the Proxy when external and Cb Server when internal.

Requirements

- Layer 7 Firewall or Proxy
- Internal DNS Server
- External DNS Server
- External and Internal IP Space

Advantages

- No additional hardware, if Firewall/Proxy supports Reverse Proxy

Limiting Factors

- Internal Cb Server open externally on SSL after full SSL Inspection on Proxy for ONLY Sensor traffic