IT Consultancy Report on
Implementing Data Intercept Technologies
for
Active Defense LLC

Prepared for
Active Defense LLC

Prepared by
Sofia Sackett
15 February 2020

I. Executive Summary

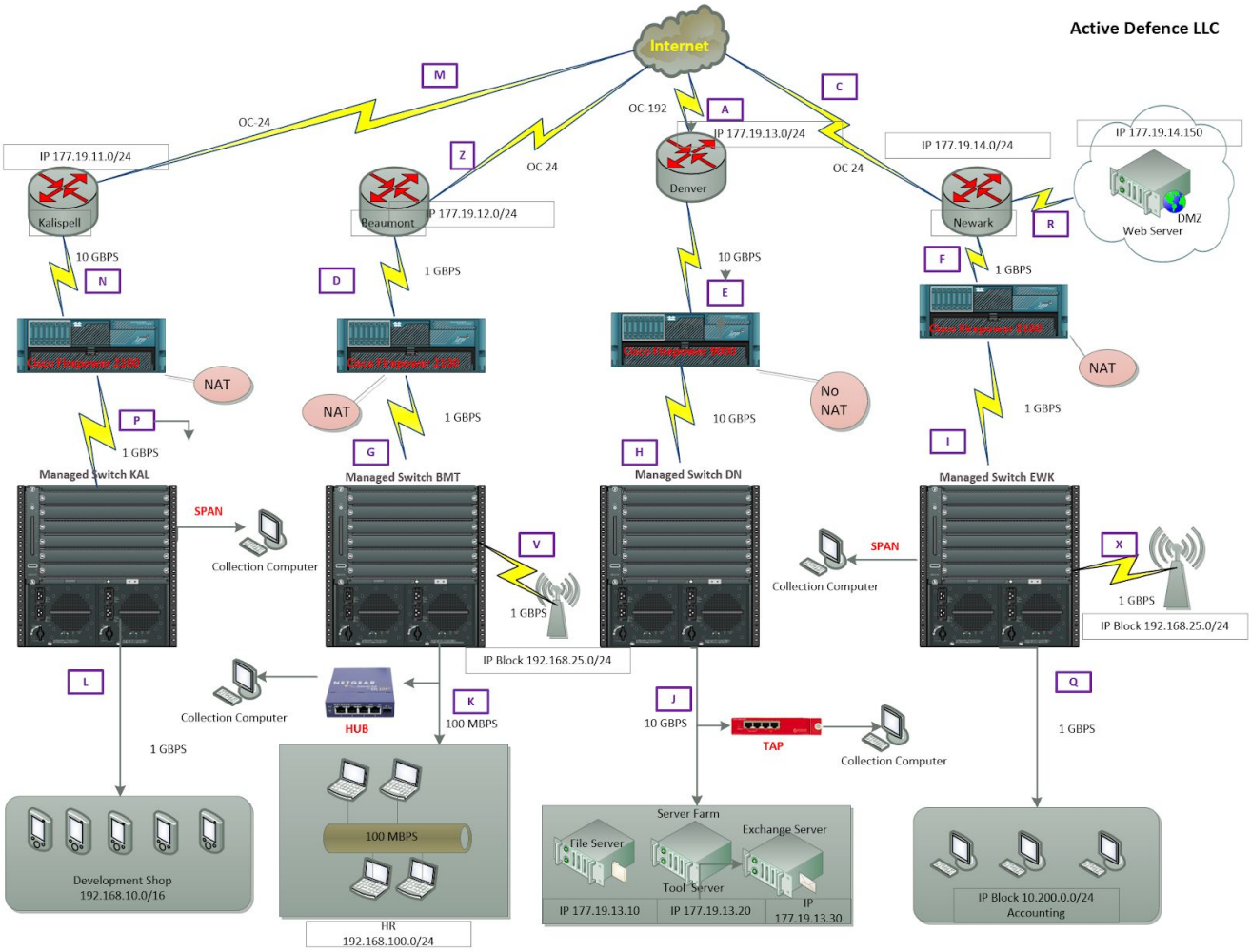
Based on the network configuration of Active Defense LLC, viable intercept methods include implementing hubs, utilizing network Test Access Ports (TAPs), and configuring Switch Port Analyzers (SPANs) on managed switches. Each of these methods is illustrated below in a network diagram. In terms of legality, Active Defense LLC has done enough legally to allow for the interception of network data from workplace computers, however more could be done to protect Active Defense when it comes to their BYOD Wi-Fi service including adding a login banner.

II. Legality

Since Active Defense LLC is a private company, the employer can consent to the search of any computer that they have provided for an employee since that computer is considered workplace property per United States v. Ziegler, 474 F.3d 1184. Therefore, as long as the appropriate manager consents to the collection of network traffic from workstations, Active Defense is legally in the clear. However, when it comes to Bring Your Own Device (BYOD) devices, Active Defense does not have the legal power to collect that traffic because those devices are not company property. Though the BYOD connections are outward-facing and therefore cannot access any of the Active Defense servers, it would still be prudent to put a login banner in place. A login banner provides a warning to users that the network they are connecting to has an Acceptable Use Policy (AUP) that users must adhere to and often requires the user to consent to being monitored in order to gain access to the network. The banner effectively removes the user's reasonable expectation of privacy and allows for the legal interception of network traffic.

III. Network Intercept Methods

The network configuration of Active Defense LLC provides three effective options for network intercept: hubs, Test Access Ports (TAPs), and Switch Port Analyzers (SPAN). The following diagram depicts each of the three possible intercept methods. The managed switches from the Kalispell and Newark offices are shown configured with SPAN'd ports as well as collection computers. Point K on the network diagram marks the best place for a hub to intercept traffic, and point J shows where a potential network TAP could be placed. All taps are placed over Ethernet connections due to their prevalence and their broadcast-based nature.



a. Implementing a Hub

Hubs are half-duplex devices and can be categorized as multi-port repeaters because, in contrast to switches, when a hub receives a packet on one port it copies the packet and sends it out all of the other ports so that the rest of the network can see the packet. Hubs are an inexpensive choice for tapping a network; however, they have a maximum throughput of 100 Mbps. As seen in the above diagram, the hub has been intentionally placed in between Managed Switch BMT (Beaumont) and the HR workstation at point K, so that the hub will not be responsible for slowing down the network speed. The hub is also connected to the collection computer and target network with Ethernet cables.

b. Utilizing a Network Test Access Port (TAP)

The network TAP was placed in between the target computers and the switch at point J between Managed Switch DN (Denver) and the server farm. This TAP was specifically situated on the Denver portion of the network because that particular firewall does not employ Network Address Translation (NAT) so we can tap as close to the target as possible. Though it has not been shown in this diagram, a regenerating TAP is the best choice for network intercept because it can send traffic out many ports; therefore, a forensic examiner could send the target traffic to multiple computers or software products at once, such as Wireshark, SNORT, and an IDS. It is also necessary to consider the layer 1 characteristics of both the target or switch and the TAP since they must have the same material, connectors, and other physical qualities in order to work together properly.

c. Configuring Switch Port Analyzers (SPANs)

SPAN, also known as port mirroring, is a feature that can be configured on any managed switch. Switch Port Analyzers send a copy of the packets received on one port (a source SPAN port) to another port (a destination SPAN port) where the traffic can be analyzed. However, one must be careful not to exceed the backplane bandwidth of the switch because it may cause dropped packets. It is also worth consideration that one should avoid tapping outside the VLAN with a SPAN because those networks are generally unable to talk to one another without the help of a router. In the above network diagram SPAN has been configured on both Managed Switch KAL (Kalispell) and EWK (Newark).