White Paper

A Fortified Sandbox

Encapsulating network traffic to protect your private network.

McAfee

Table of Contents

Overview

McAfee® Advanced Threat Defense enables organizations to detect advanced targeted attacks and convert threat information into immediate action and protection. Unlike traditional sandboxes, it includes additional inspection capabilities that broaden detection and expose obfuscated threats.

Detection of zero-day malware is facilitated through a multi-layer approach. With the combination of multiply down select engines, including antivirus signature detection, real-time emulation, and dynamic analysis (sandboxing) to analyze actual behavior. In addition, the use of full static code analysis is leveraged to provide detection capabilities of even the most evasive and advanced malware. By unpacking the malware and exposing the assembly code, true static code analysis is able to be performed. This allows McAfee Advanced Threat Defense to remove obfuscation techniques to expose the original executable code for analysis of all attributes and behaviors of the intended behavior of the payload.

This paper discusses the ability for McAfee Advanced Threat Defense to preform advance detection measures to convict zero-day threats and advanced evasive malware while preventing the propagation of malware or malicious activities from the sandbox to one's private network. By fortifying the sandbox through the network layer, encapsulation of network traffic is achieved and prevention of infiltration of malware can be carried out while advanced detection capabilities are triggered to understand the full behavioral intent of malware. Thus, elevating concern of malicious files and exploitation infiltrating into your secure private network.

Malware Internet Access

Deployment of McAfee Advanced Threat Defense (ATD) provides a centralized sandbox solution with the ability to provide vector agnostic threat detection through a multitude of down select engines native to ATD. As the malware is propagated to ATD for analysis, and the file is sent to be detonated within the sandbox for dynamic and static code analysis, the option to enable malware internet access can be chosen. The purpose of this functionality is to fully understand the behavior of the malware, and to align it with any known malicious behaviors or familial classifications based on the observed behavior during sandboxing. Allowing the sample to reach outside the network can provide additional awareness of its behavior. For example, the malicious intent of the malware may be to reach out to a command and control server calling for an asymmetric encryption key which begins to restrict access of data on a system. Providing such a comprehensive retrospective analysis results in higher efficacy of detection of malicious intent of a malware in question.

But with such a feature at the disposal of potentially harmful malware, how does a sandbox restrict the propagation of network traffic to the internal network in which it's been implemented to protect from such threats?

Deployment Considerations

The sandbox can be placed within a demilitarized zone (DMZ), or placed strategically behind a firewall to ensure restricted network access to other vectors. Use of a DMZ is done to provide further segregation of a wide area network (WAN) from the local area network (LAN). While the DMZ can provide an additional layer of security of network traffic which is internet-facing, it can potentially put a security solution in a vulnerable area to be targeted to malicious activities such as a Denial of Service (DoS) attack on the network services. By deploying ATD within a DMZ, the exposure to an unprotected external network can lead to vulnerabilities being leveraged to disrupt the appliance. This could be in the form of the aforementioned DoS attack, for example on HTTPS services for ATD once the attacker has uncovered the public IP address associated with the sandbox. The outcome is a less than optimal deployment within the network topology of the sandbox solution.

While this can be a functional solution, the architectural deployment may not be optimal, and further resources must be shuttled into to deploy the sandbox in such a fashion resulting in a less than ideal scenario. Fortunately, ATD is engineered to address this issue and solves the problem of stopping network traffic from being monitored on the malware interface, and restrict traffic from entering the management interface of the appliance.

Network Encapsulation

To achieve a secure deployment of ATD outside the boundaries of a DMZ, ATD provides host network services for the analysis virtual machines (VMs) which allows network traffic isolation to the designated network interface card (NIC). Two network interfaces which are present is the management interface, and the malware interface. While the management interface governs the majority of network activity, the malware interface will provide a tunnel to the external network for malware analysis occurring during dynamic and static code analysis. Enabling samples being executed for analysis to access network services, the observation of network activities of the sample can be accomplished. A software emulated network interface is provided for the VMs on the kernel level.

Network Simulator

A software emulated network interface is provided for the VMs on the kernel level. This internally emulated network allows the sandbox environments to stimulate network services. Observable network traffic is kept isolated to each VM through a kernel firewall, keeping network services initiated in one sandbox environment from propagating outside of its own internal network. Traffic will also be routed to a default gateway address, which does not exist on the internal network but rather is set as a simulated default route by the Network Simulator. To encapsulate network activity to each VM, and prevent overflow outside of the virtualized sandbox, a network drive is provided to each analyzer that secures and isolates traffic to the singular VM.

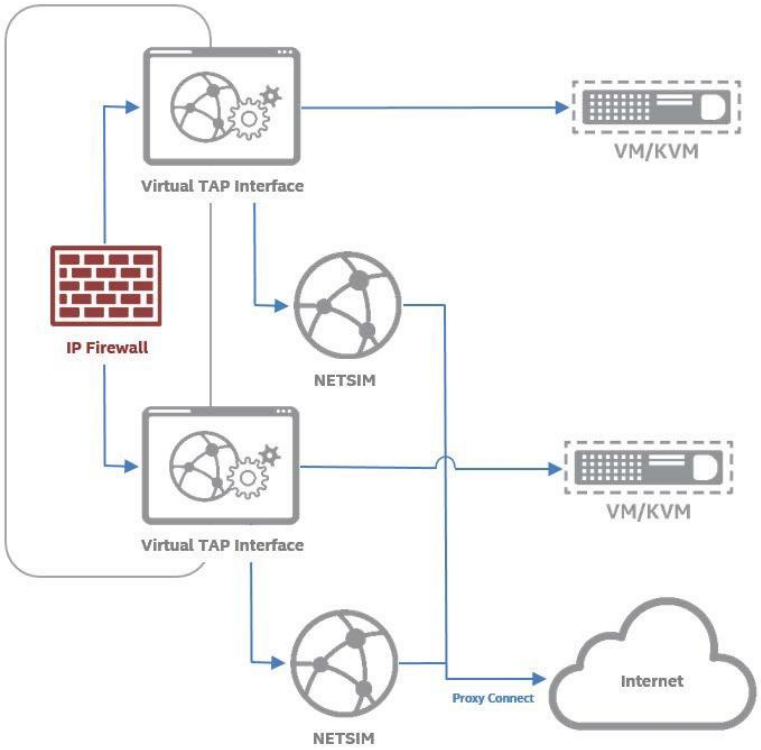

Figure 1. A network diagram providing a workflow of the encapsulated network traffic through the Network Simulator.

The Network Simulator will initiate emulated services on a host and only one instance of the Network Simulator will be bound to the network interface of each analysis subject. This is set in such a way that the operating system subject has its network configured to use this network interface as a default route for all external connection attempts. This allows the Network Simulator to capture network activities and services. Once network activity has been captured by the Network Simulator, a log file is produced containing any captured network traffic. The network capture will be aggregated into an analysis report, after which the logs will be purged and the Network Simulator will await a new connection for the next analysis to take place. By utilizing the Network Simulator, an internal firewall, and network drive, each VM which is created to detonate a sample within its sandbox will self-contain the network traffic, not allowing traffic to reach other network services outside of the encapsulated environment.

Live Internet Option

McAfee Advance Threat Defense can be configured to access live internet using a secondary network interface called a malware interface. Some of the advantages of using live internet are, downloading and analyzing of additional payloads, discovery of any DNS or IP redirects, and validation of an attacker's infrastructure. The use of a Dirty Network is recommended when configuring the malware interface. A "Dirty Network" is either a direct connection to the internet or an area with internet access that has no other corporate assets in it. Any assets in the dirty network could be compromised by the executing malware. ATD also provided the ability for the malware interface to use a separate DNS. It is also recommended to use a separate DNS as attackers could learn the DNS used during the malware analysis. The diagram below highlights a typical deployment of the malware interface.

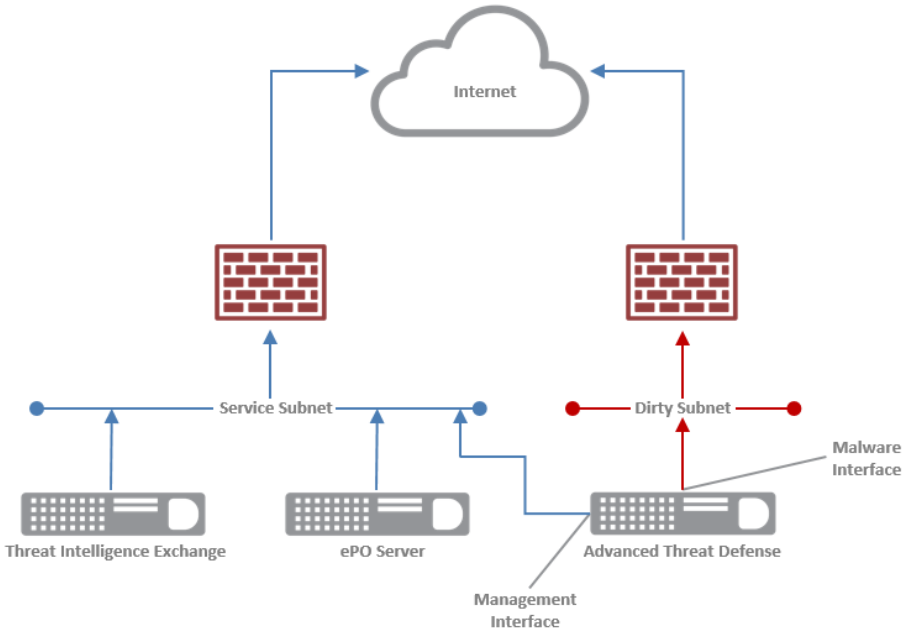

Figure 2. A network diagram providing a workflow of egress traffic via the Management Interface and the Malware Interface.

Complementary Network Architecture for an Optimal Sandbox

McAfee Advanced Threat Defense provides emulated Internet services to potentially malicious malware. Providing the simulated services through the Network Simulator, and providing the ability for the malware to still interact through real services. Exposing DHCP and DNS services to VMs, and providing a specified IP to allow the necessary access to the internet, but behavioral observation of the network services called upon by the malware can be observed to ensure increased efficacy of detection.

Architecting network services provides an outcome of a further fortified sandbox which is intelligently designed to go beyond signature less detection, and arch into advanced dynamic and static code analysis. Expanding past local host activity, and into network services to capture he full scale of the malicious intent of malware. Whilst insulating the payloads within the sandboxes from reaching critical and sensitivity segments of a network, resulting in an optimal sandbox that is sure to meet the requirements for detection capabilities.

McAfee LLC
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com