|  |
| --- |
| Blue Team |
|  |

# Create Best Practice Security Profiles for the Internet Gateway

To: IT Director

From: FROM

We have implemented the recommended best practice settings for each security profile on the Palo Alto firewall. Here is a quick summary of the rules that we have implemented.

1. Antivirus Profile
   1. The antivirus policy will scan all traffic coming through the firewall and will prevent viruses and malware from being transferred over HTTP, SMTP, IMAP, POP3, FTP, and SMB.
2. Vulnerability Profile
   1. The vulnerability profile rules will protect against attacks such as buffer overflows, illegal code execution, and other client and server-side vulnerabilities. It will drop all client or server packets that have a severity of critical, high, and medium. It will apply the default rules to packets that have vulnerabilities of informational or low.
3. Anti-Spyware Profile
   1. The anti-spyware profile will drop all traffic that is suspected of reaching out to a command-and-control server. This will help keep compromised hosts from establishing malicious outbound connections, and will help identify compromised hosts. The anti-spyware profile will also sinkhole known malicious domains.
4. URL Filtering Profile
   1. The URL filtering profile will block traffic to web content that is likely to have malicious content. It will block all malicious content. This includes command-and-control, copyright-infringement, dynamic-dns, extremism, malware, phishing, proxy-avoidance-and-anonymizers, unknown, newly-registered-domain, grayware, and parked. The URL filtering rule will also alert on all categories of malicious content.
5. WildFire Profile
   1. The WildFire profile will help protect against unknown threats. The WildFire profile sends all traffic in both directions to WildFire for analysis.
6. File Blocking Profile
   1. The file blocking profile we are using is the predefined strict file blocking profile. This policy will block all batch files, DLLs, Java class files, help files, Windows shortcuts (.lnk), BitTorrent files, .rar files, .tar files, encrypted-rar and encrypted-zip files, multi-level encoded files (files encoded or compressed up to four times), .hta files, and Windows Portable Executable (PE) files, which include .exe, .cpl, .dll, .ocx, .sys, .scr, .drv, .efi, .fon, and .pif files. This rule will also alert when all other files are transferred to increase visibility across the network.
7. Security Profile Group leveraging all above Best Practice Profiles
   1. We have created a security profile group that has all of the above Best Practice Profiles
8. Security Profile attached to all Security on the firewall
   1. The above security profile group has been attached to all firewall rules