|  |
| --- |
| Team 14 |
|  |

# Memorandum

To: Management

From: Team 14

Date: February 18, 2023

Subject: Inject Name

Palo Alto’s IPS features include filtering network traffic by inspecting packets as they pass through the firewall. When inspecting the packets, Palo Alto can examine what application is communicating, in addition to what port and protocol it is using. Many of our security policy rules are filtering based on application.

In addition to this, we have configured security profile groups for the following categories:

* Antivirus
* Anti-Spyware
* Vulnerability Protection
* URL Filtering
* File Blocking
* WildFire Analysis
* Data Filtering
* DoS Protection

These security profiles are configured according to Palo Alto’s recommended best practices, found here: <https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/create-prisma-access-policy/security-profiles/security-profile-best-practices>

All of these policies are packed in a security profile group. This security profile group is being applied to all security policies.

The following pages have screenshots documenting our security configuration. Feel free to reach out with any further questions or comments.

Thanks,

Team 14

Image 1: description