Network Intrusion Prevention System (IPS)

The ability to monitor network traffic is a key component of protecting Fpweb.net's information systems. Even still, defending those systems from the many threats can be a daunting task. A firewall is commonly used to provide a layer of security for its respective local network. Firewalls by themselves have limitations though. Most can only block based on IP addresses or ports.

In contrast Network Intrusion Prevention Systems (IPS) is able to use signatures designed to detect and defend from specific types of attacks such as denial of service attacks among others.

Prevention Methods

1. Auto Update IPS Signatures through Cisco.com.
2. Monitor logs and IPS attacks through Monitoring software.
3. If an attack is happening the IP address is blocked for 2 days in an ACL on the firewall preventing all traffic from the IP into Fpweb.net's network.
4. If the attacker tries again from that IP after it has been allowed back the IP address will be permanently blocked from all traffic into Fpweb.net's network.
5. If the server is compromised all ports on the switch to the customer server is shut down until the server is cleaned and passed Fpweb.net's security team.
6. If the server cannot be cleaned a restore will take place back to before the attack and the vulnerability patched before put back into deployment.

Fpweb.net IPS System Diagram

Fpweb.net's IPS Systems sit inline before traffic reaches the customers server as seen below.