Tech Brief

DomainTools

Importing Custom Blocklists into Popular Security Controls

Revised June 2022

Background

When threat hunting, incident response investigations, automated enrichment, or other SOC or intel center actions produce customized lists of domain or IP indicators, these may be of interest to teams administering security controls such as firewalls, email security proxies, web proxies, EDR, etc. Many popular vendors have provisions to ingest customized blocklists, but it is not always easy to find instructions for doing so. This document is offered as a reference for those interested in ingesting such lists into their controls.

***NOTE*: vendors change their product functionality over time, so the links provided here may become obsolete.** *They have been verified as of the Updated date on the cover page of this document.*

NGFW/Perimeter Security/Cloud Proxies

Cisco NGFW (IP addresses only)

Palo Alto Networks

Juniper SRX: Overview | Example

Fortinet FortiGate

Check Point

WatchGuard IP address | DNSWatch

Zscaler Single | Bulk

Email Security

Cisco ESA (This specifically documents configuring a Host Access Table, which is the relevant part of a custom blocklist rule)

Proofpoint

Microsoft Forefront TMG

Symantec Email Security

McAfee Email Gateway (NOTE on scalability: this documents a one-at-a-time GUI for adding blocked domains)

Websense/Forcepoint

Barracuda (see particularly Example 2)