Configure Security Policy

- Change Security Policy app rule to "Application Default"
- Will work more with Shad on this

Configure Application Filter

- Objects > Application Filters > Add
  - Name
  - Category:
    - 64 Collaboration
    - 227 general-internet
    - 49 media
    - 89 networking
  - Subcategory:
    - 27 Audio-streaming
    - 227 file-sharing
    - 22 gaming
    - 44 proxy
    - 45 remote-access
    - 64 social-networking
  - Technology
    - 228 browser-based
    - 146 client-server
    - 3 network-protocol
    - 52 peer-to-peer
  - risk:
    - 3, 4, 5
  - Characteristic
    - 279 Evasive
    - 218 Excessive Bandwidth
    - 172 Prone to misuse
    - 111 SaaS
    - 368 Transfer Files
    - 105 Tunnels Other Apps
    - 150 Used by malware
    - 343 Vulnerability
    - 313 Widely Used

Configure Antivirus Profile

- Objects > Security Policies > Anitvirus
  - Name
  - Antivirus
    - Check Packet Capture
  - Click Ok

Configure Antivirus Profile

- Objects > Security Policies > Anti-Spyware
- Rules
  - Name
  - Threat name = any
  - category = any
  - action = reset both
- DNS Signatures (DNS Sinkhole)
  - Sinkhole IPv4 = random dead ip
  - Sinkhole IPv6 = IPv6 Loopback IP (::1)
  - packet capture = extended-capture
  - Click enable pass DNS monitoring

Configure Vulnerability Protection Profile

- Objects > Security Policies > Vulnerability Protection
- add
- name
- Host Type = client/server (Repeat rule again for both)
- Action = Block IP
- Duration = 600
- packet capture = extended-capture
- Severity = critical, high (Repeat rule again for both for low aswell)

ACC Tab

Use ACC tab to export network data

Configure Wildfire

- Device > Setup > Wildfire
- Make sure it is enabled
- Objects > Security Profiles > File Blocking
- Ensure best practices is enabled
- (You can leverage this in security policy rule under Actions < Profile setting < File blocking)

griffins files

.exe .bat .com .cmd .msi .msp .js .vbs .ps1 .php .jsp .zip .rar .tar .tz .7z .tar.gz .tgz .ini .conf .cfg .sql .sh .bat .bak .htaccess