



# Firewall Logs and Configs

THREAT MANAGEMENT

# Firewall Logs and Configs

- Both firewall and router logs and configurations indicate accepted and blocked connections
- It is a good way to passively understand your network design
- Reading configurations is quicker than “reverse engineering” the log files



# Firewall Logs

- Often use log levels to categorize information and debug messages
- Cisco, Palo Alto, and Check Point all log things a little different, but have common items
  - Date/Time Stamp
  - Details of the event
- Logs are designed to be human readable
- Access logs on Cisco using “show logging” command



# Example Firewall Logs

Feb 2 12:15:04 192.168.0.1 %ASA-5-710003:  
User &apos;ASAadmin&apos;; executed the  
&apos;enable&apos;; command

[https://www.cisco.com/c/en/us/about/security-center/  
identify-incidents-via-syslog.html](https://www.cisco.com/c/en/us/about/security-center/identify-incidents-via-syslog.html)



# Example Firewall Config

ip access-list extended inb-lan

permit tcp 192.168.0.0 0.255.255.255 any eq 22

permit tcp 172.16.0.0 0.15.255.255 any eq 22

permit tcp 10.10.0.0 0.255.255.255 any eq 22

deny tcp 192.168.1.0 0.255.255.255 any eq 22

It can help to read these to yourself like this:

“Allow tcp traffic from 192.168.0.0 to any destination IP on port 22”

