CCDC Inject

INJECT NAME	Logging Denied FW Packets
INJECT ID	SOCS03A

INJECT DESCRIPTION:

An important component to security operations is to review network traffic that was denied by the firewall to discover reconnaissance activity, or failed attack/intrusion attempts.

INJECT DELIVERABLE

Develop a business memo that describes what configuration elements of the FW cause denied packets to be logged. Include a snapshot from the most recent 30 minutes from logs that illustrate denied packets being rejected at the FW. Also, provide an analysis of the most recent 30 minutes of log entries as to if they represent reconnaissance or intrusion attempt activity.