CCDC Inject

INJECT NAME	Finding Internal Network Rogue Packets
INJECT ID	SOCS01A

INJECT DESCRIPTION:
The CISCO is concerned about intra-segment network traffic within our internal network. There are some potential future applications that will require some measure of isolation and the potential of a machine becoming compromised on one of our segments being able to mount attacks on machines on other segments needs to be addressed.

Identify the capabilities in our existing infrastructure that will allow us to limit inter-segment packet flows to only those that are expected and log those that are no expected. We can then use those logs, of unexpected packets, to identify potential malware or otherwise compromised machines. Implement this solution.

INJECT DELIVERABLE
Respond with a business memo that describes how we might configure our existing infrastructure to meet this goal with evidence for it's implementation.