



# CCDC Inject

<b>INJECT NAME</b>	FW Packet Capture & Analysis
<b>INJECT ID</b>	TOOL10T

## **INJECT DESCRIPTION:**

Using the PA Firewalls packet capture tool: capture packets between one of your Windows Servers and an external address. Decode the captured packet in Wireshark and describe what the captured packets represent (ex: TCP connection for SMTP etc...) Also explain to management how this feature can be useful, under which circumstances.

## **INJECT DELIVERABLE**

Respond with a business memo that specifically addresses:

- 1.) Screen captures of the PA packet capture configuration rules.
- 2.) Screen capture of the Wireshark screen showing the decoded results and describe what they represent in terms of protocol and application function.
- 3.) Statement to management as to the benefits of this FW feature. Provide a scenario in which this could be useful.