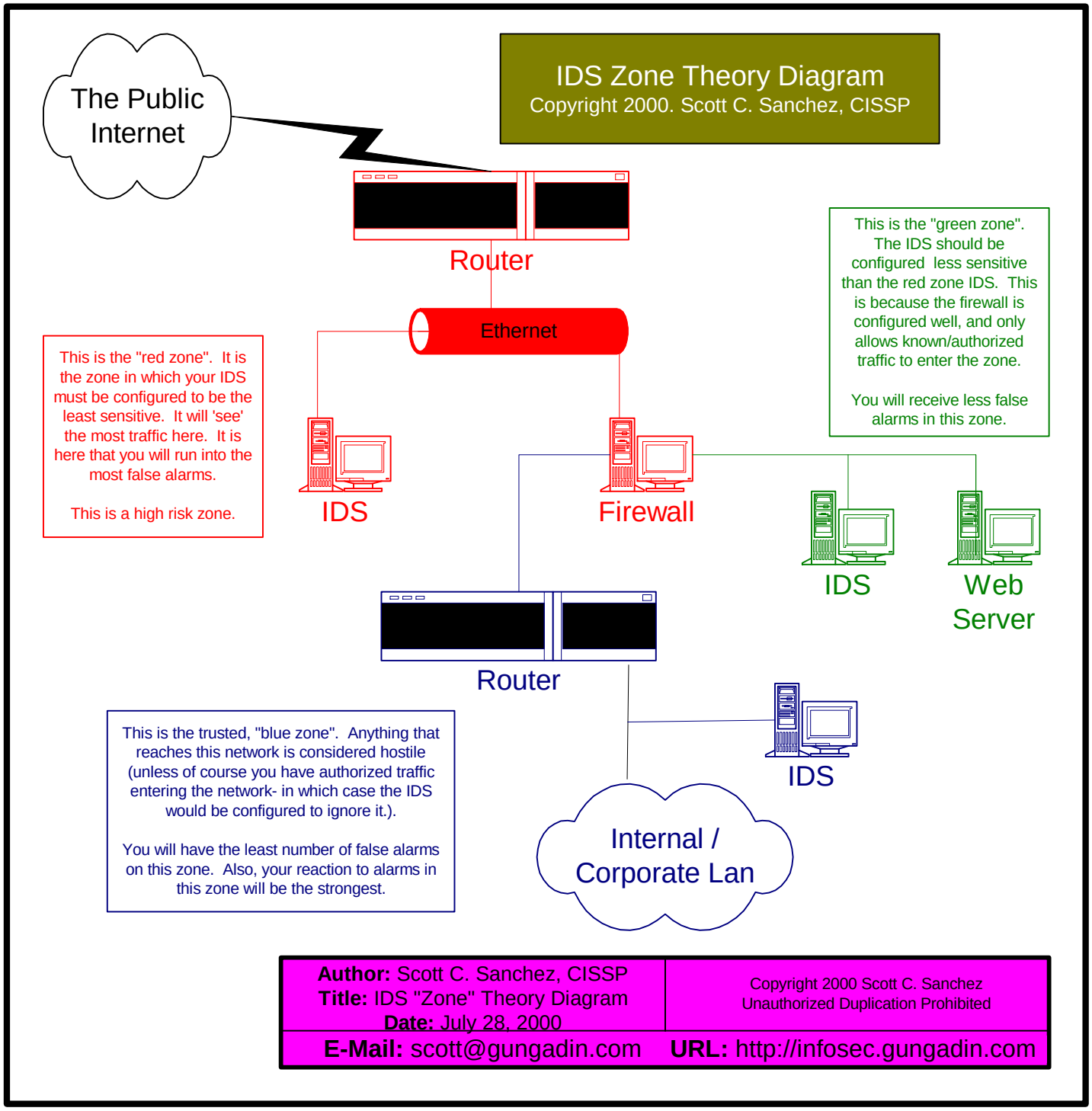
IDS Zone Theory Diagram
Copyright 2000. Scott C. Sanchez, CISSP
The Public Internet
Router
Ethernet
This is the "red zone". It is the zone in which your IDS must be configured to be the least sensitive. It will 'see' the most traffic here. It is here that you will run into the most false alarms.
This is a high risk zone.
IDS
Firewall
This is the "green zone". The IDS should be configured less sensitive than the red zone IDS. This is because the firewall is configured well, and only allows known/authorized traffic to enter the zone.
You will receive less false alarms in this zone.
IDS
Web Server
Router
This is the trusted, "blue zone". Anything that reaches this network is considered hostile (unless of course you have authorized traffic entering the network- in which case the IDS would be configured to ignore it.).
You will have the least number of false alarms on this zone. Also, your reaction to alarms in this zone will be the strongest.
IDS
Internal / Corporate Lan
Author: Scott C. Sanchez, CISSP
Title: IDS "Zone" Theory Diagram
Date: July 28, 2000
Copyright 2000 Scott C. Sanchez
Unauthorized Duplication Prohibited
E-Mail: scott@gungadin.com
URL: http://infosec.gungadin.com