

Platform Hardening



**Part 2: What do we need to do and
How do we need to prepare to Harden systems**

CONTACTS

- ✘ Michael Gough – CISSP, CISA, VP ISSA Austin
 - + Senior Risk Analyst - Comptroller of Public Accounts
 - + Author – ‘SkypeMe!’ and ‘Video Conferencing over IP’ by Syngress Press
 - + Contributor to the Center for Internet Security Benchmarks.



AGENDA

- ✘ Part 1 – *What* is Platform Hardening and *Why* do we have to do it
- ✘ Part 2 – *What* do we need to do and *How* do we need to prepare to Harden systems
- ✘ Part 3 – *How* to Harden (Win, *NIX, Cisco, Handhelds)

WHAT

- ✘ Do we need to do to prepare to harden?

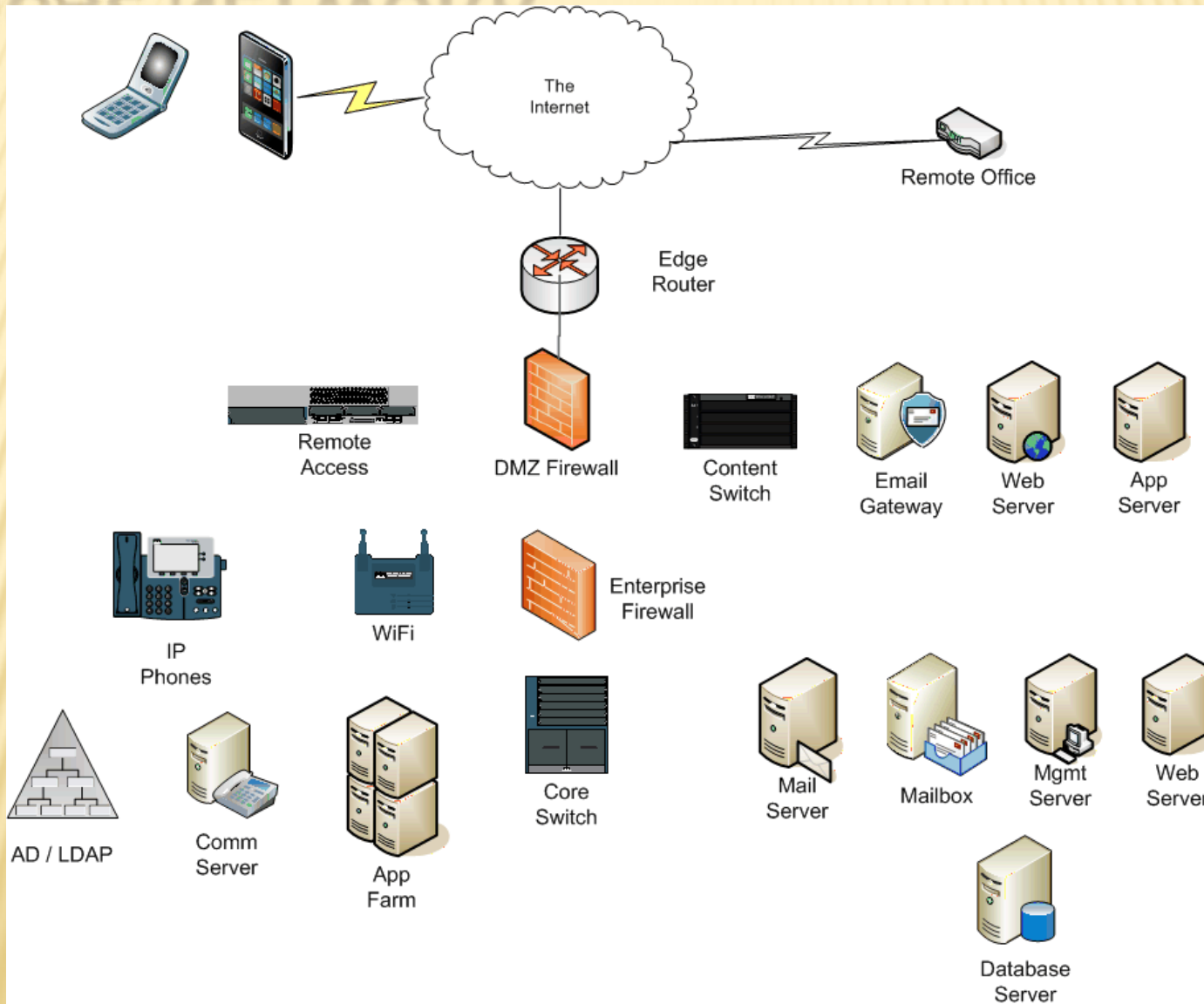
COMPLIANCE

- ✘ The first thing to do is decide what we are trying to comply to...
 - + Sarbanes Oxley
 - + HIPPA
 - + PCI
 - + IRS 1075 (SCSEM)
 - + FISMA – NIST 800-53
 - + TAC / TGC
 - + ISO 17799/27001
 - + Your own Policy, Standards & Guidelines....

PLATFORMS



TYPICAL NETWORK



BEFORE YOU BEGIN

- ✘ You can't know the extent of your problem...
- ✘ Unless...
- ✘ You know what you have!

KNOW WHAT YOU HAVE

✘ Some call this Asset Management



✘ I call this....

+ Solar Winds



+ NMap



+ Special scripts

✘ Find your Windows, Unix, Printers, Network devices and populate a database

KNOW WHAT YOU HAVE

- ✘ Use your own security suave to find, locate and document your own list of items.
 - + Create a Spreadsheet or Database
- ✘ Yes, you can use your list to verify what Asset Management “thinks” they have.
- ✘ But we security sluths can query services, daemons, etc., find everything Asset Management does not know about...