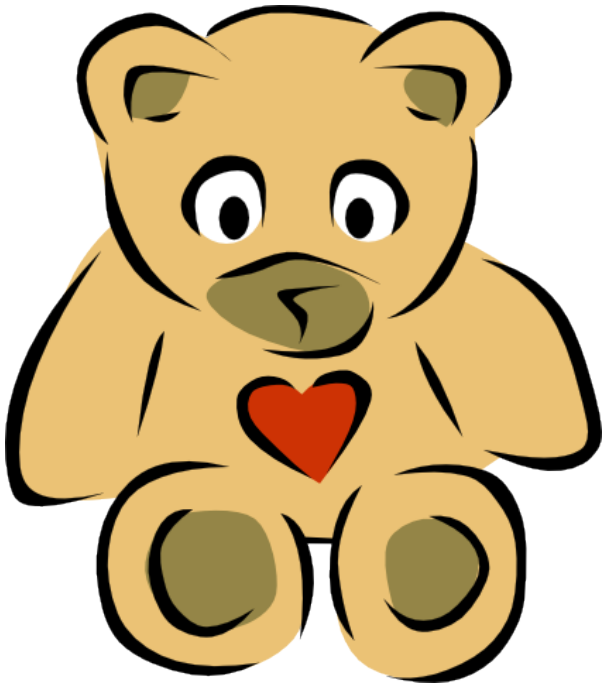
Firewalls



Why do people want a firewall?

- “[...] a firewall’s purpose is to keep the jerks out of your network while still letting you get your job done.”
- “[Limiting] what kinds of connectivity is allowed between different networks.”
  - Internet Firewalls: Frequently Asked Questions

- Very vague, no specifics!

Definition of “*Firewall*”

Must:

- Block at least some network traffic
- Allow through at least some traffic

(More on NAT later)

The “*Crunchy Shell*” model

- End of 1980's ~ 2000's
  - No internal software upgrades
    - Manual upgrades too costly – no good automation available
  - Strict firewalls as only protection
    - Strict division between *internal* and *external*
  - “Crunchy shell around a soft, chewy center”

1420

The “*Crunchy Shell*” model

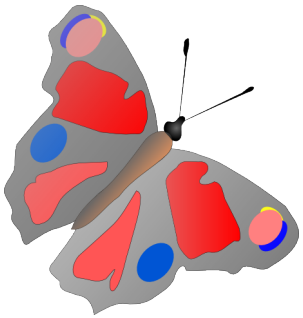
- Economic reasons no longer valid!
  - Automated tools now available
  - Thin clients

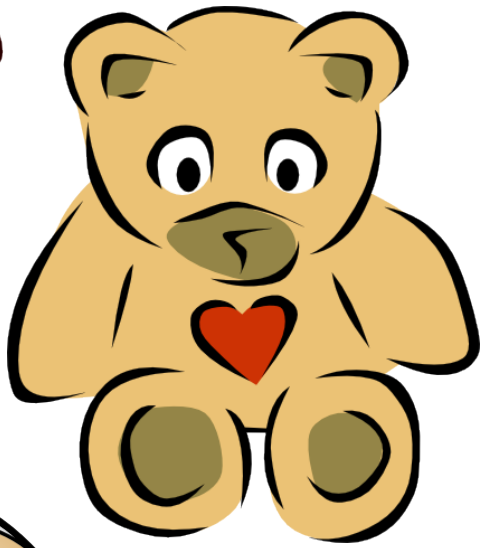
Package management and update systems

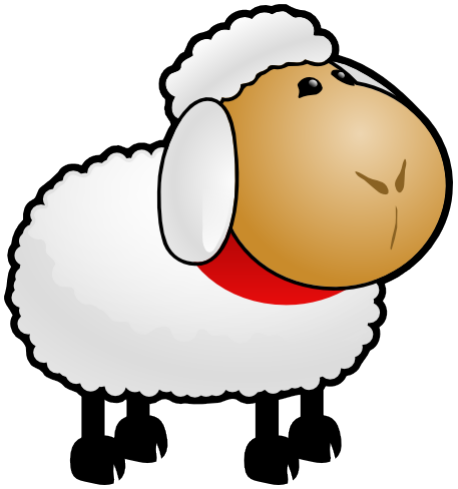
APT, YUM, Windows/Microsoft Update, etc.

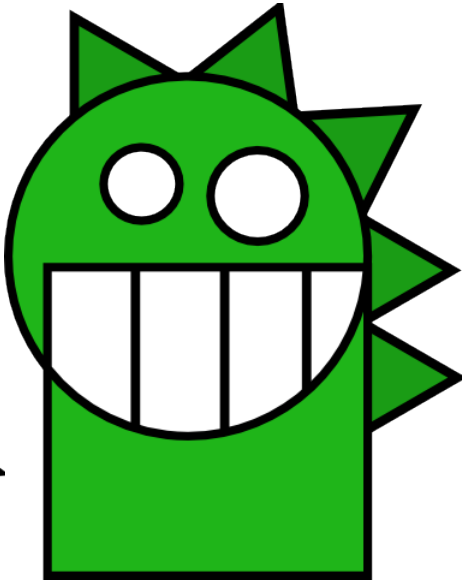
Cloning/System image systems

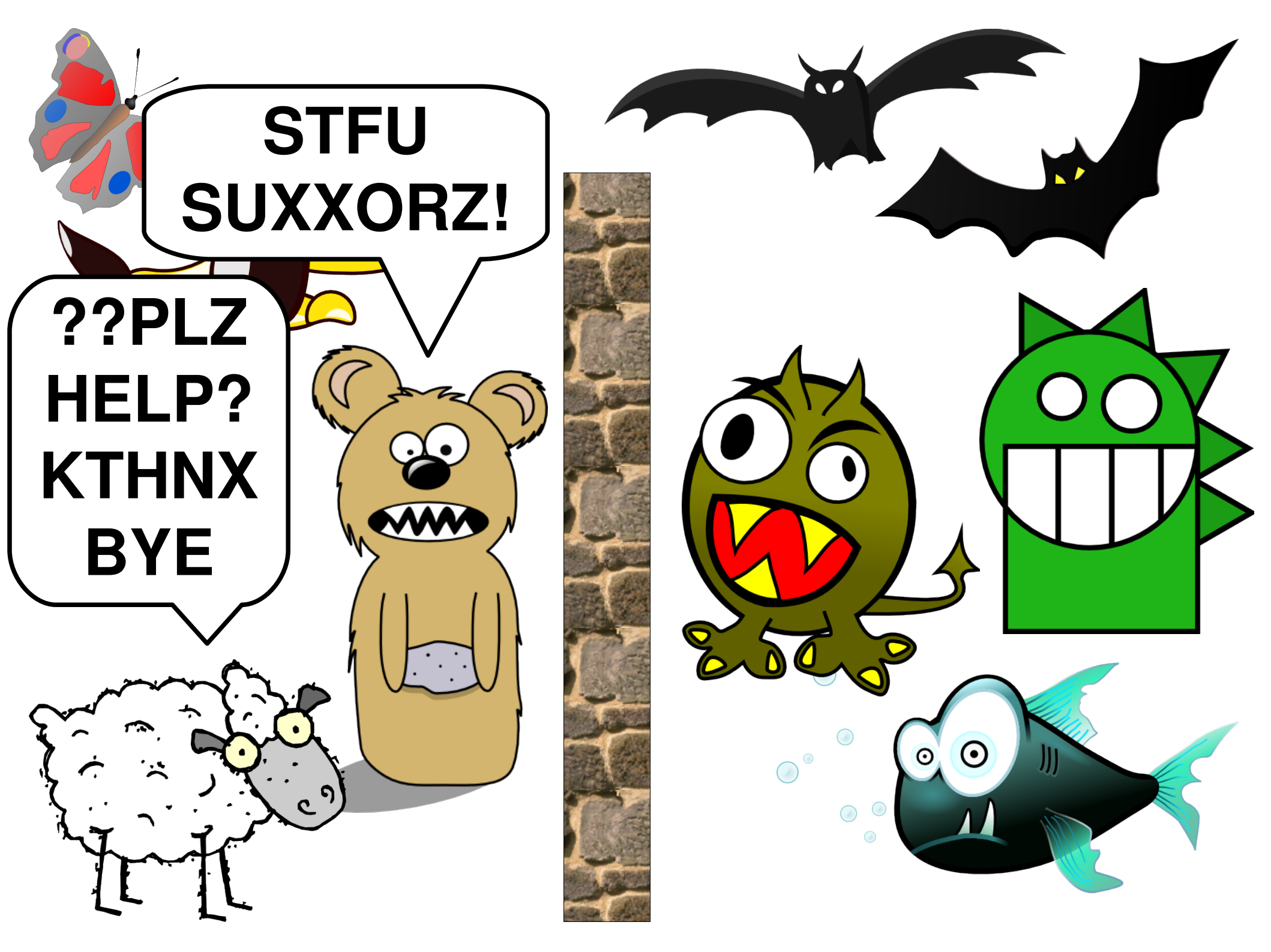
Ghost, SystemImager, etc.

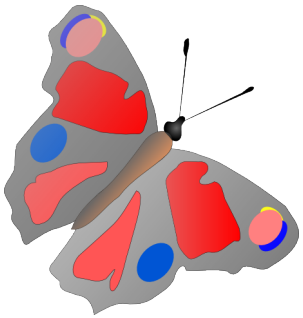


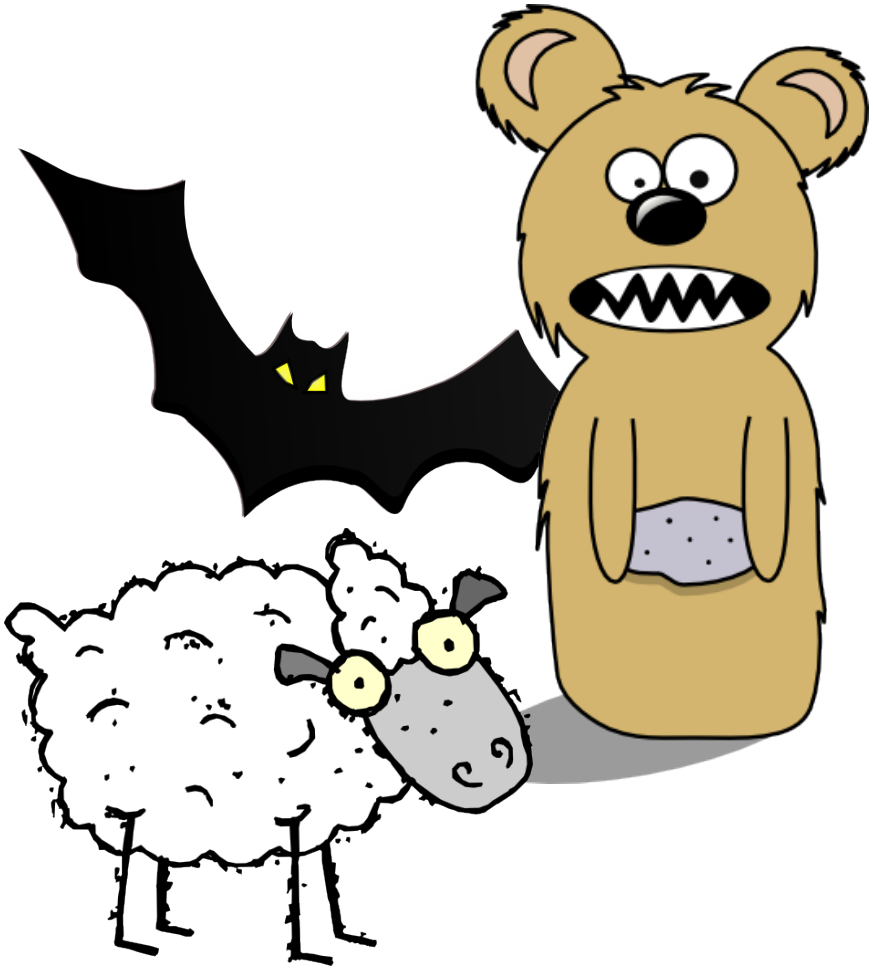







STFU
SUXXORZ!
??PLZ
HELP?
KTHNX
BYE





The “*Crunchy Shell*” model

- **Insiders larger threat than all external threats combined**
  - Information security breaches survey 2006
- **68% of companies reported losses from insider threats**
  - CSI/FBI Computer crime and security survey 2006

The “*Crunchy Shell*” model

Conclusion:

- Security model simplistic and outdated

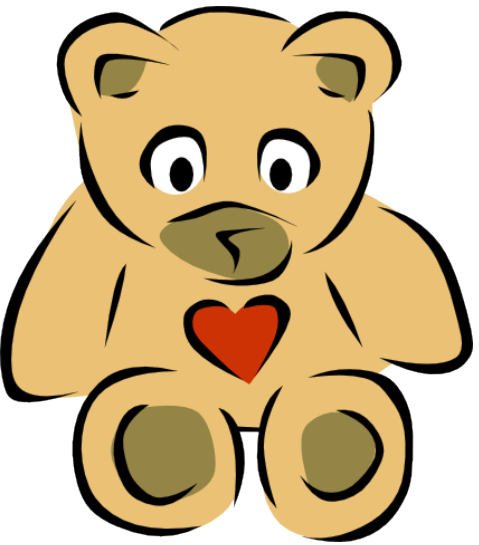
The “*DMZ*” model

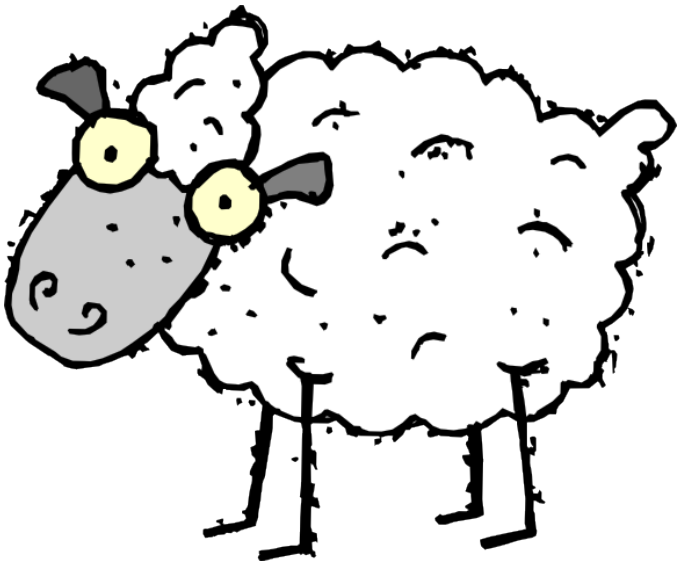
A.K.A. the 3-legged model

- DMZ created as an improvement to the “Crunchy Shell” model

- “Black and White” became

  “The Good, the Bad, and the Ugly”

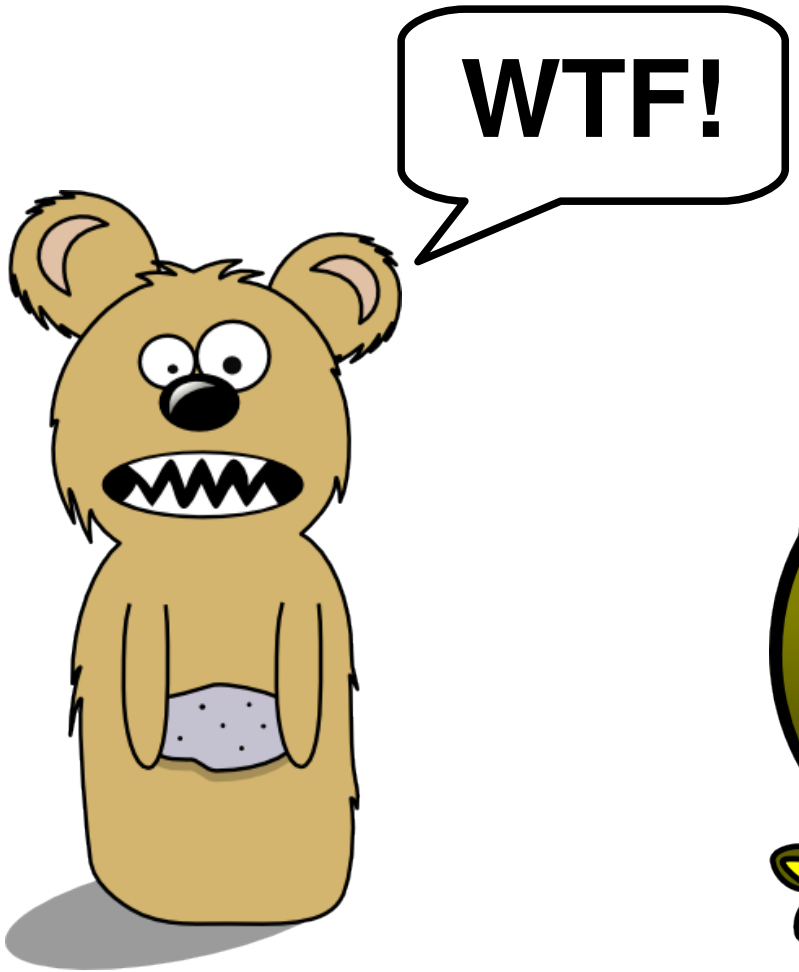


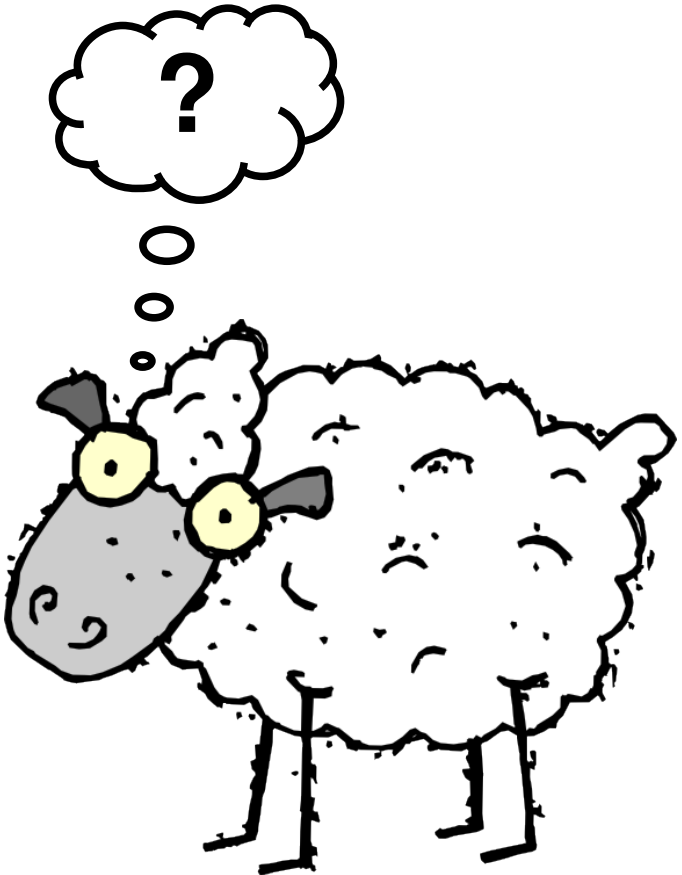


The “*DMZ*” model

A.K.A. the 3-legged model

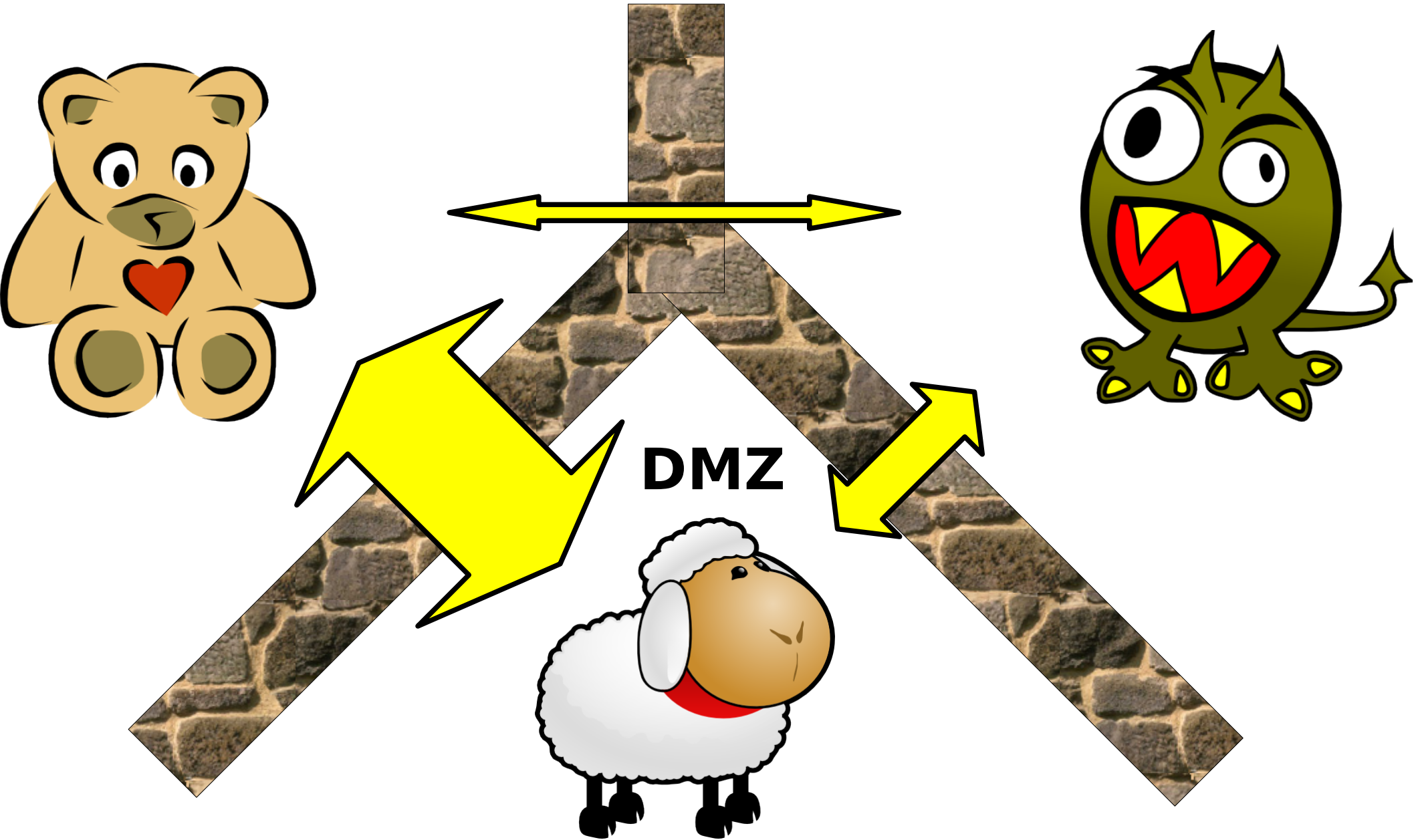
- Security model still simplistic!





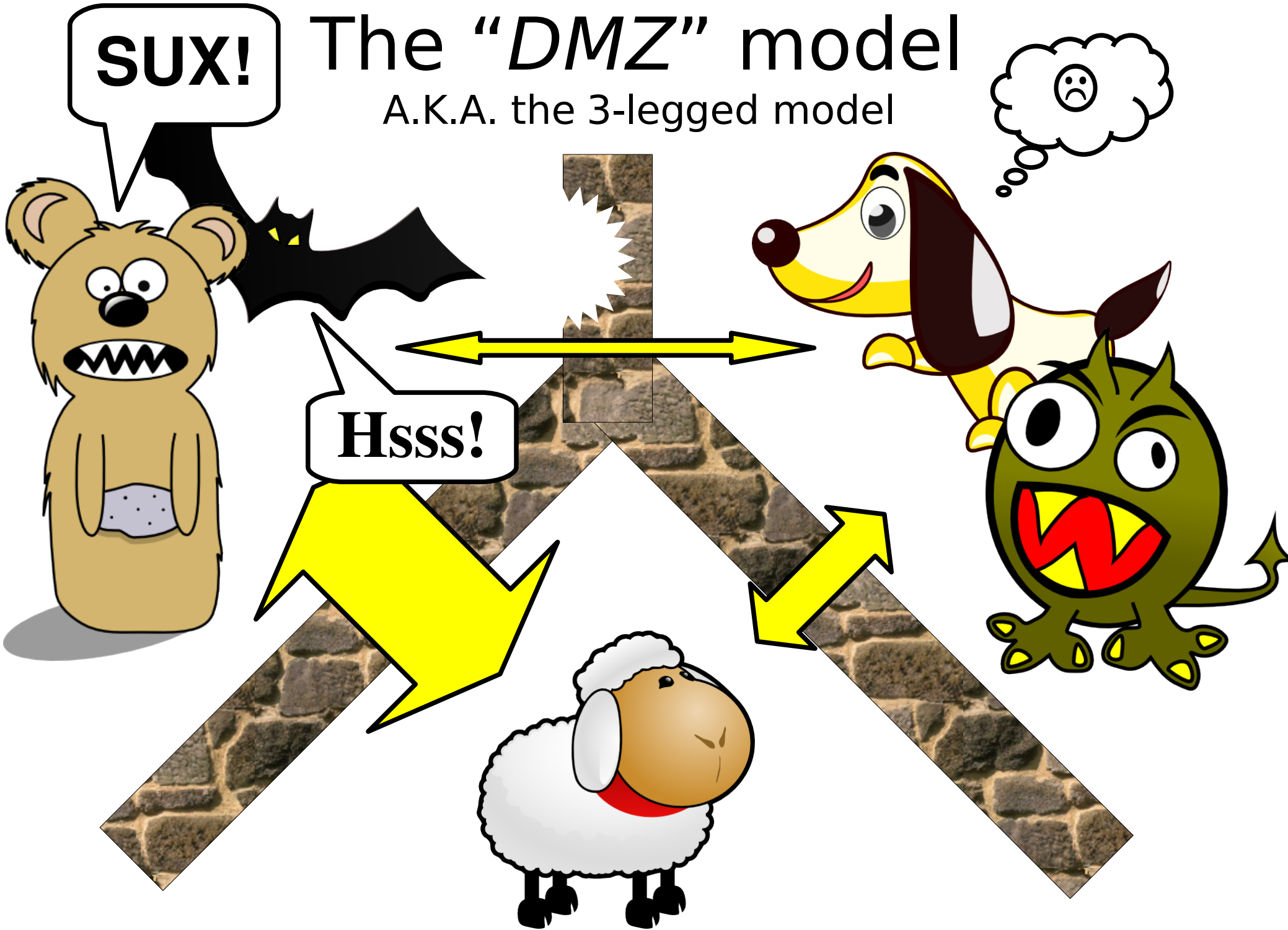
The "*DMZ*" model

A.K.A. the 3-legged model



The "*DMZ*" model

A.K.A. the 3-legged model

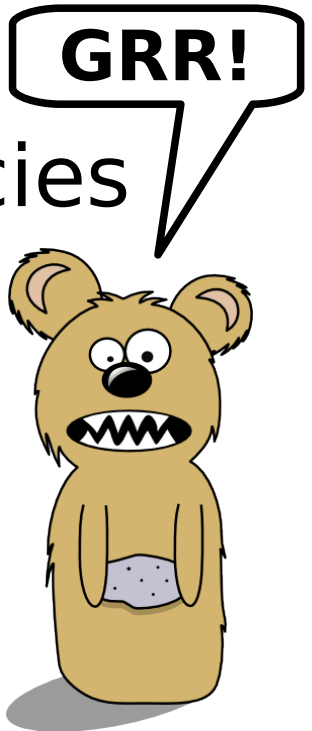


A firewall should not be noticed

A visible firewall will be circumvented in ad hoc ways, for *good reasons* by users with *legitimate needs* for doing so.

This:

- Teaches user to ignore security policies
- Breaks network monitoring
- Creates antagonistic users (☹)
- ***Weakens security***



- The introduction of a firewall and any associated tunneling or access negotiation facilities MUST NOT cause unintended failures of legitimate and standards-compliant usage that would work were the firewall not present.
  - RFC 2979

Two models

- To construct a firewall:
  - Explicit Permit
  - Explicit Deny

Explicit Permit

- Aggravates users
  - Transparency loss?
- Easy breaks functionality of the network
  - Black hole routers
  - Complex network communication
    - Multilayer games, telephone system
    - Distributed/redundant systems
- Causes lots of network problems
  - IT support commonly asks you to turn off all firewalls as a first recourse

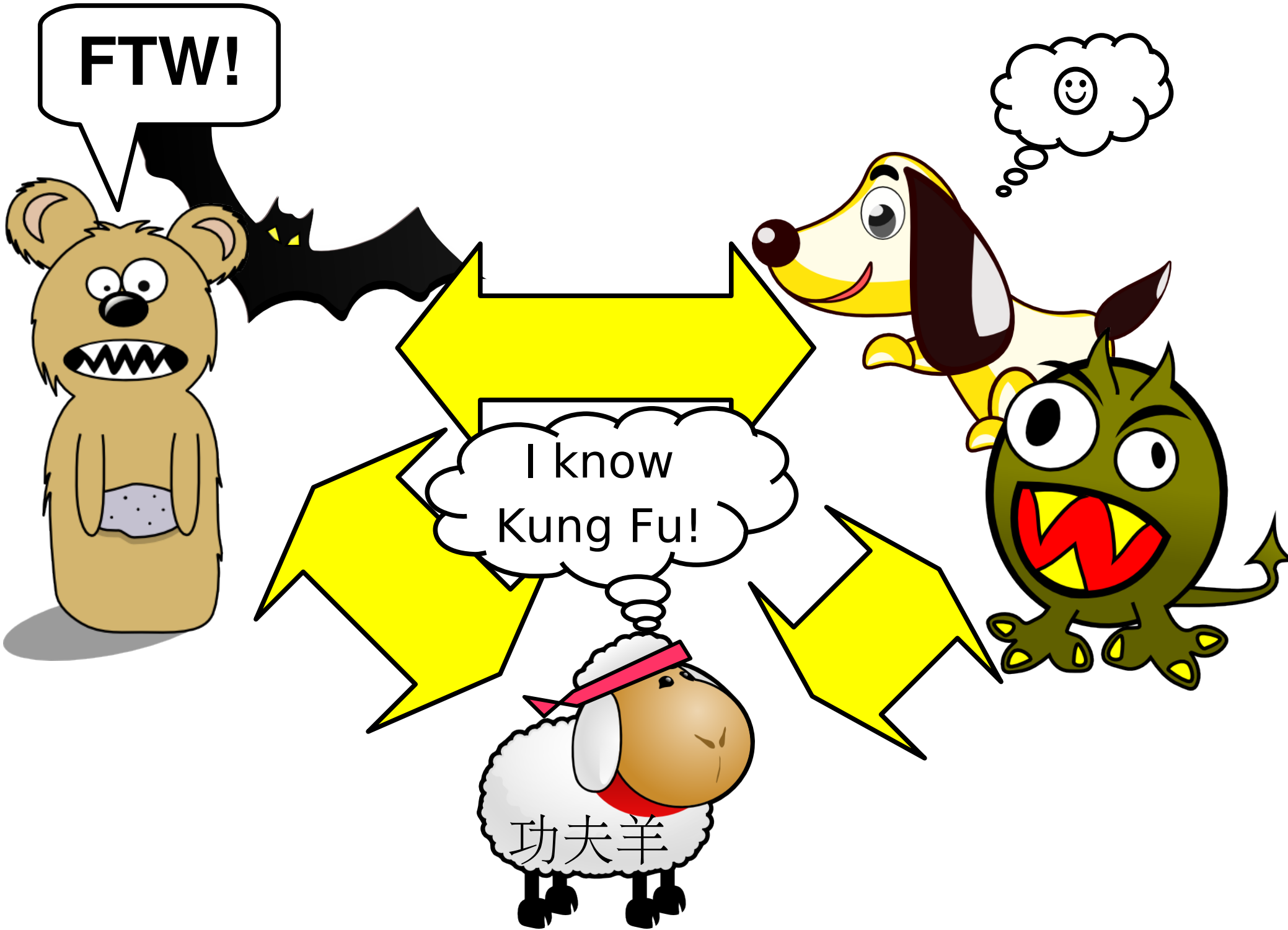
Explicit Deny

- Loss of any specific use
  - If you know the problem, why not update?
- Problematic to convert policy guidelines to firewall rules
  - Wording like “stop all outsiders”
- Larger configuration files

What to do then?

- Maintain your firewall rules!
  - Both models demand constant maintenance in production.
    - Explicit permit is not a substitution for maintenance
- Combine Explicit deny with Explicit permit
  - Block all from a specific units in the network
    - Trust?
- Know the effects of any single block!

- Everything over HTTP: port scan attacks occur frequently in today's Internet, looking for open TCP or UDP ports through which to gain access to computers. The reaction from computer system management hasbeen to close down all the unused ports, especially in firewalls. One result of this reaction is that application designers have moved to transporting all data communications over HTTP to avoid firewall traversal issues. Transporting "everything over HTTP" does not block attacks but has simply moved the vulnerability from one place to another.
  - RFC 4948 (August 2007)


FTW!
I know
Kung Fu!
功夫羊

NAT

Network Address Translation

- Internet is designed as a peer to peer network
  - Anyone can directly contact anyone else
- No distinction – except bandwith – between a home user and a large corporation.
- Two factors came to oppose this:
  - Address shortage
  - ISPs wanting more restricted consumers

NAT

- Common ISP terms-of-service agreements *prohibit any kinds of servers!*
- Access deals where servers are allowed are in most cases too expensive for the individual user
- This creates a direct class distinction:
  - Those who can use the Internet freely by running web servers, etc
  - Consumers, who can only buy services, "*The Firewalled Consumer*"
    - "*The Digital Imprimatur*", John Walker, 2003

NAT

- “NAT has several negative characteristics that make it inappropriate as a long term solution, and may make it inappropriate even as a short term solution.”
  - RFC 1631 (May 1994), “The IP Network Address Translator (NAT)”, written just as NATs were beginning to be used more widely.

NAT

- “NAT breaks a fundamental assumption of the Internet design; the endpoints are in control.
- Another design principle, ‘keep-it-simple’ is being overlooked as more features are added to the network to work around the complications created by NATs.
- In the end, overall flexibility and manageability are lowered, and support costs go up to deal with the problems introduced.”
  - RFC 2993 (Nov 2000), “Architectural Implications of NAT”

Further reading

- Rethinking the Design of the Internet, M. S. Blumenthal, D. D. Clark (2000)
- RFC 2979, Behavior of and Requirements for Internet Firewalls (October 2000)
- RFC 3724, The Rise of the Middle and the Future of End-to-End (March 2004)