Are Firewalls Obsolete? The Debate

Pro: Marcus J. Ranum

Con: Marcus J. Ranum

1

Firewalls are Dead

- Opening Position:
  - Firewalls are a **kludge** - ***let's have real network security instead!***
  - New services and increasing interconnectedness of everything defeat the design of firewalls
  - Firewalls don't really solve anything - ***they just give warm fuzzy feelings!***

2

Long Live Firewalls!

- Opening Position:
  - Firewalls continue to be necessary because the standard software base simply isn't good enough to withstand attack - ***and the situation isn't getting any better!***
  - Firewalls draw a useful boundary between interconnected networks
  - In many cases a firewall is the only protection a network can have

3

Firewalls: too Expensive

- Managing a firewall is a headache
- $15,000 and up for a firewall is ***absurd***
- Vendors and consultants cannot justify expense in terms of actual value provided by product
- As 'net evolves we need to replace our $15,000 firewalls every 3 - 5 years

4

Firewalls: Costly?

- Average cost for damage control of security incident is $100,000*****
- Some sites report losses (in time, opportunity, business) over $1,000,000*****
- Replacement cost and rate for firewalls is comparable to other computing devices: who is still using *386/33s* which cost $2,000 4 years ago?

*source: CSI Poll

5

Interference Unwelcome

- Firewalls block valuable services and reduce utility of the ‘net
- Whenever a new service is invented the firewall needs to be reconfigured
- Firewalls are a tremendous impediment to achieving electronic commerce or the kind of collaborative environment the Internet was intended to be

6

Firewalls? Intrusive?

- Not all firewalls are intrusive
- The problem is not really the firewall it is the application
  - Reasonably designed applications can support firewalls
  - Some applications can gain performance and ease of use benefits from firewalls (e.g.: firewall + web caching proxy)

7

Software Security

- Newer Internet-ready software has security built in (e.g.: Netscape +SSL)
- Operating system security is improving
  - Windows NT is C2!
- What we really need to do is keep fixing the software base rather than refusing to communicate

8

Software? Secure?

- Pick your favorite nightmare:
  - "Installed Base"
  - "Legacy Systems"
  - "Backwards Compatibility"
- As for system software security:
  - It takes ***one*** hole in ***one*** system and it's all over
  - Newer O/S' like NT will have new bugs

9

My Router is Enough

- For performance reasons a firewall is impractical
- If I configure my router correctly I can get adequate security if I know what I'm doing
- Since there is new software coming out all the time the only thing I ***know*** can handle it is my router

10

Enough Routers

- A router that is correctly configured to provide security ***is a firewall***
- Performance concerns are a real consideration
  - If you're concerned about the performance of your firewall then buy a fast one
  - In the future networks and systems will be faster and so will firewalls

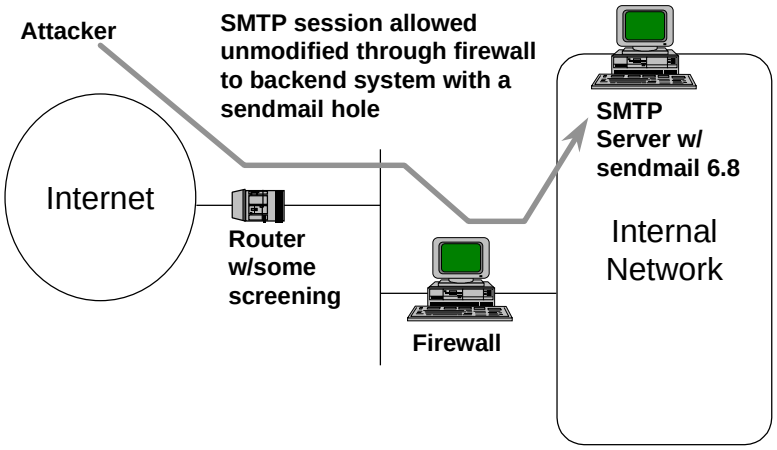
11

Incoming Traffic

- Data streams that are allowed in by firewalls may not be protected
- Some firewalls perform application specific security on data streams
  - Others do not
  - Sometimes you can't
- Splits security between firewall and system on backend

12

Incoming Traffic *(cont)*



13

Incoming Traffic

- This ***is*** a serious problem
- Incoming traffic reduces to a software security problem on the host
  - Any software where you're providing an interesting or significant service should be appropriately protected

14

What Perimeter?

- Firewalls assume that there is a “boundary” of some sort around the network
  - Not all networks have clear enforceable boundaries
  - Some networks are too big
- Need a firewall at each entry/exit point
  - This sells a ***lot*** of $15,000 firewalls!

15

Perimeter Erosion

- Don’t blame the firewall if your network doesn’t have a perimeter
  - It is a policy and network design problem
  - It shows ***past*** lack of concern about security
- As networks evolve there will still be administrative boundaries (of some sort) between them

16

Viruses

- In the future viruses and attack programs are likely to be an even greater threat than they are today
- Firewalls don't stop viruses
  - And they aren't going to!

17

Viruses

- Firewalls are not the correct tool for virus-proofing
  - Virus scanners are
- Don't blame firewalls for not blocking viruses
  - That's like complaining because your car is a lousy can-opener

18

Java and Applets

- Firewalls' answer to Java and applets is to block the applet
  - That's not ***real*** security!
  - That's not an adequate response in the long term
- If (when?) computing becomes increasingly applet/browser based firewalls become irrelevant

19

Java and Applets

- This is a ***serious*** problem
  - Firewalls at least may provide an impediment to attackers that are exploiting a successful attack program or applet
  - Damage containment

20

Not ***Real*** Security

- Firewalls are counter-evolutionary
  - They let us hunker down helplessly in dark corners rather than facing the problem and developing real security solutions
- Firewalls are basically a form of denial exercise
  - The ‘net equivalent of sticking our fingers in our ears and screaming ***“Go Away!”***

21

Real Security

- People were in denial long before there were firewalls!
- Researching the next generation of security tools is for researchers not people with production networks
  - Let the people with real work to do hunker down
  - Let the researchers research

22

IPV6

- IPV6 with encryption and security options will make firewalls obsolete
- Everything will be Virtual Private Network(VPN) based and encrypted
- Hackers will no longer be able to sniff or intrude without access to cryptokeys
- Firewalls will go away and we'll dance on their graves

23

IPV6

- IPV6 standard for security is likely to be delayed (more) (it's already been ages)
- Software will not be quickly deployed
  - In some cases never
  - Export control
- Worst of all IPV6 doesn't address transitive trust and operating system bugs

24

What About the Future?

- It is clear that the network is getting more complex
- It is clear that firewalls are getting very complex as well
- We're about ready for the firewall paradigm to shift

25

What About the Future?

- It is clear that there will always be administrative boundaries between networks
- It is clear that there will always be something to enforce those boundaries
- There will always be firewalls
  - They're going to evolve

26

Summary

- Firewalls not a solution for the future
- Firewalls barely a solution for today
- What we need is better software not more expensive artificial walls
- All that firewalls and firewall builders know how to do is say "***don't allow this!***" and "***don't do that!***"

27

Summary

- Firewalls are not a panacea
- Firewalls are a useful technology
- We need to combine firewalls with better host/application security
- There are some things it may never be safe to do over the 'net
  - Wanting something badly enough doesn't necessarily make it so

28