WINDOWS 7/2008 FIREWALL ESSENTIALS

The Third In a Series On Firewall Fundamentals

Carl Ness | Information Security Officer | ISPO

October 12, 2011

AGENDA

- Recap of Episode 1 & 2
- Overview of the Windows Firewall
- Important Components
- Gotcha's
- Questions and Vague Answers

IN LAST WEEK'S EPISODE…

- TCP/IP basics
- Network Architecture 101
- Netmasks & CIDR
- Stateless packet filters
- Stateful firewalls
- OS X firewall basics
- Lion's ipfilter and app firewall
- Lion's network-level firewall
- How to break into Fort Awesome

WINDOWS FIREWALL

- It is…
  - A stateful packet filter
  - A port-based firewall
  - An application firewall
  - Free
  - On by default
  - Good
  - IPv6 aware
- It is not…
  - Intuitive
  - Infallible
  - Locked
  - A spam filter
  - A phishing filter
  - A network firewall
  - OS X or *nix

IMPORTANT COMPONENTS

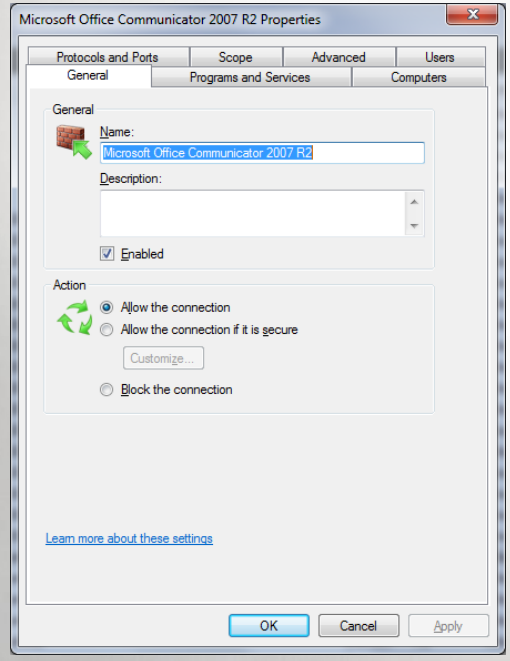
- Network Location (Profile)
- Rules are directional & can be Allow or Block
- Precedence
- Granular settings
- Program or Service
- TCP or UDP Port

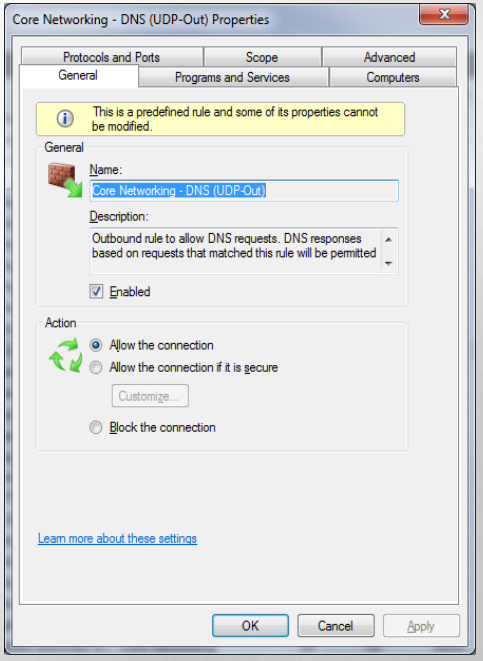
PROFILES

- Domain
- Public
- Work/Home/Private
- All

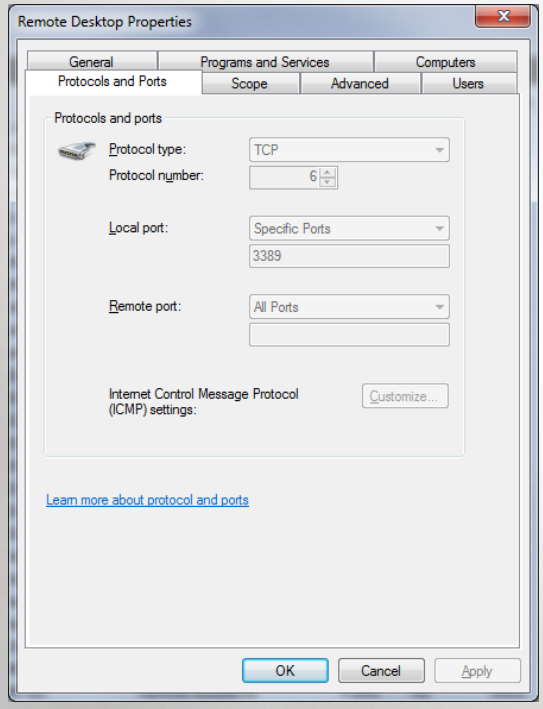
- What are these?!
- Why do we need them?
- What is enabled?
- Who's on First?

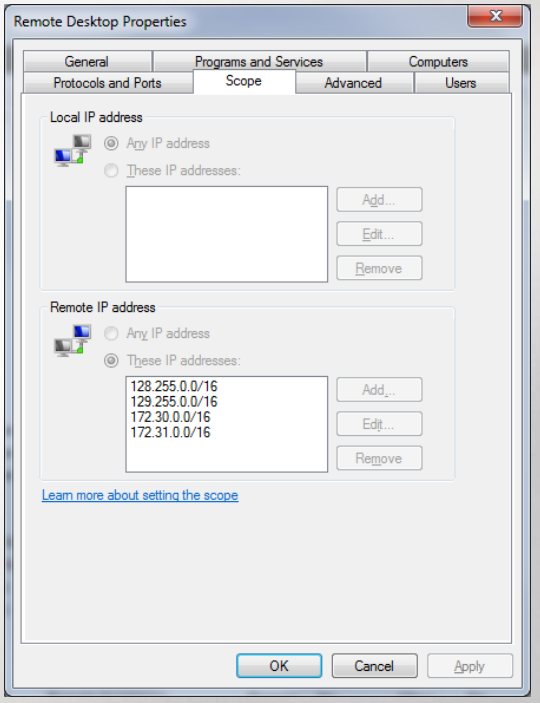
BASIC RULES


Microsoft Office Communicator 2007 R2 Properties
Protocols and Ports
Scope
Advanced
Users
General
Programs and Services
Computers
General
Name:
Microsoft Office Communicator 2007 R2
Description:
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
Learn more about these settings
OK
Cancel
Apply

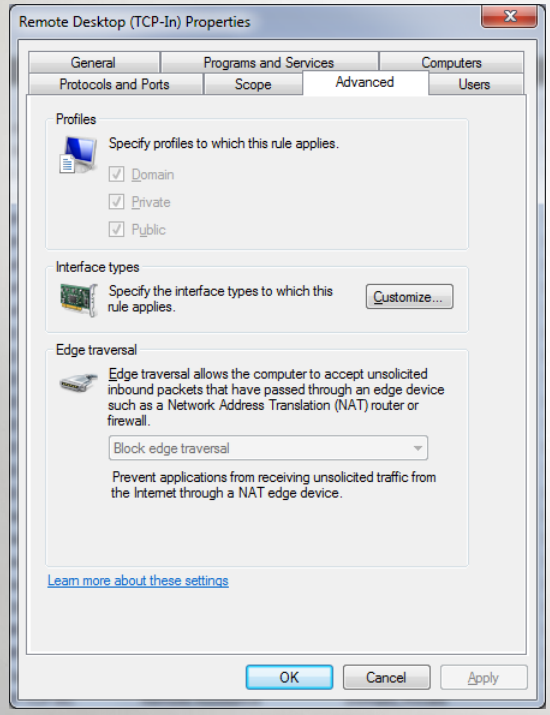

Core Networking - DNS (UDP-Out) Properties
Protocols and Ports
Scope
Advanced
General
Programs and Services
Computers
This is a predefined rule and some of its properties cannot be modified.
General
Name:
Core Networking - DNS (UDP-Out)
Description:
Outbound rule to allow DNS requests. DNS responses based on requests that matched this rule will be permitted
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
Learn more about these settings
OK
Cancel
Apply

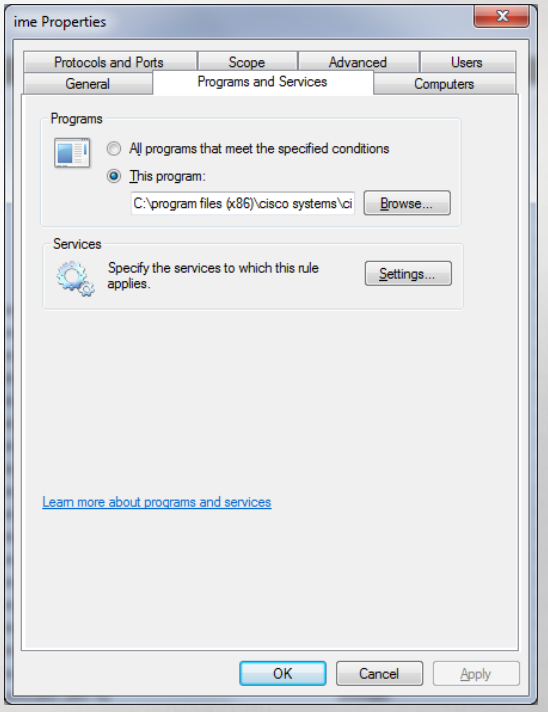
BASIC RULES #2



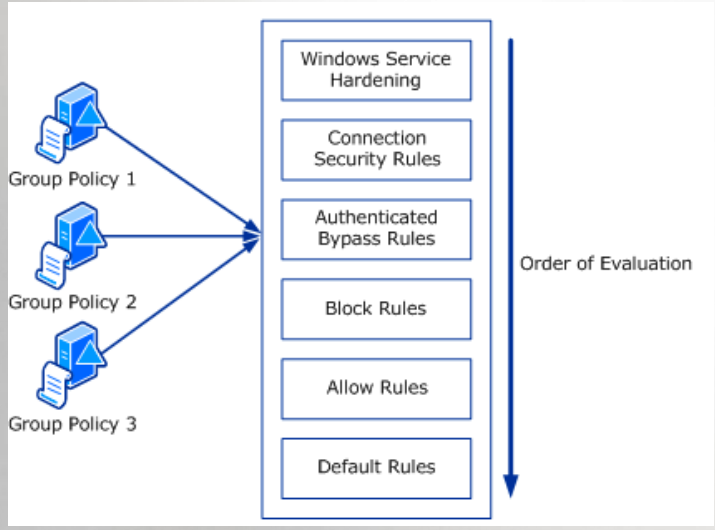


BASIC RULES #3





WHO WINS?



- Rules aren't numbered
- Default = Profile Rule
- Note Auth (IPSec) bypass
- Explicit > Any

THE NASTY BITS

- Test your settings (especially set via GPO)
- Know your applications (More on that later)
- Dual Stack
- Wireless interfaces and 6to4 tunnels
- Why, exactly, are there outbound rules, anyway?

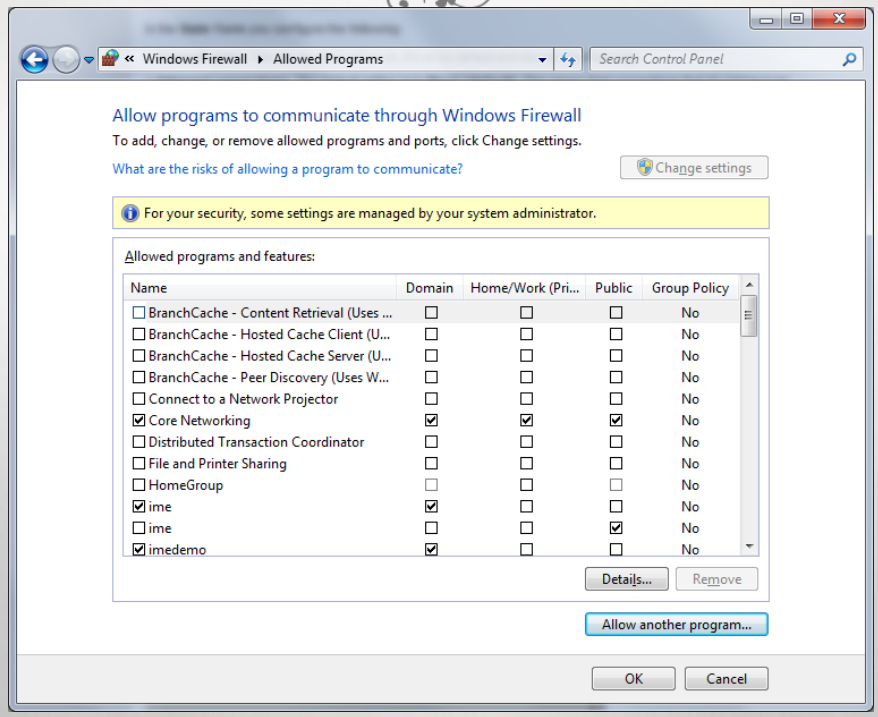
WHAT AN ID10T WILL DO TO A FIREWALL

- Local rule can override a GPO
- Users can disable the FW rule if you let them
- Users can create rules unless you lock them out
- X program not working? Disable the FW!

APPLICATIONS HATE SECURITY

- Just-make-it-work-installers
- Remember: Installers run as Administrator
- Can expose services to the world
- Tend to override restrictive rules
- New adapter? Reset Button (VMware)
- We've seen application rules that happily ignore the GPO
- Beware of GPO collisions

STUPID FIREWALL TRICKS

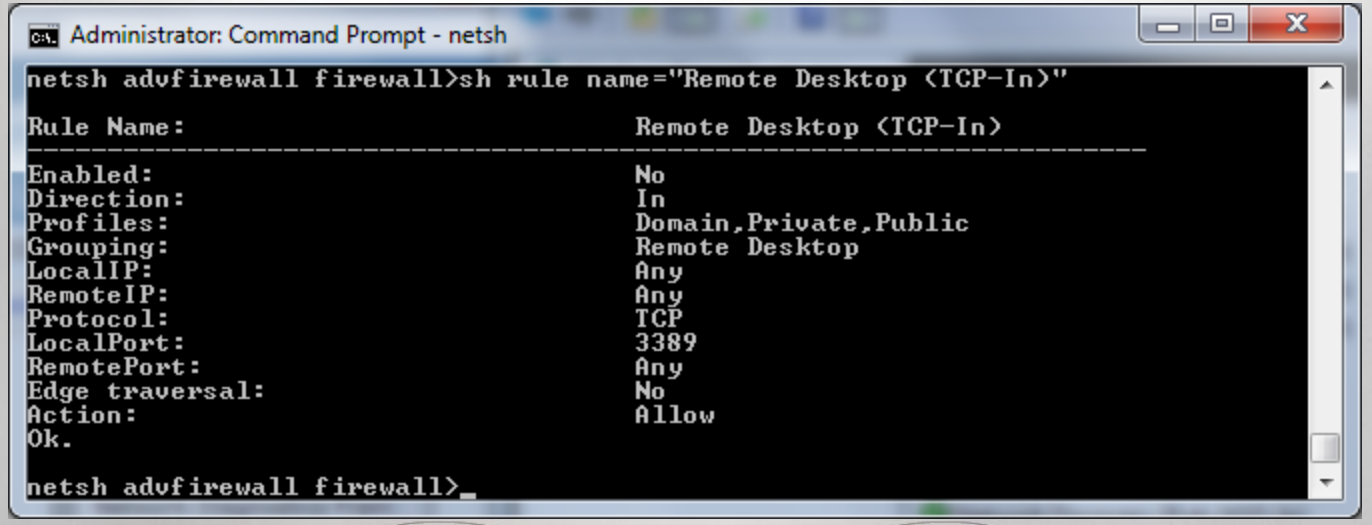


FIREWALL EXPORTS

- Firewall Export.xlsx

DON'T LIKE GUI?

- Don't forget the command line!



WE CAN HELP!

- Can review firewall settings with you
- Scan from campus
- Scan from off-campus
- ITS can provide GPO help
- Point you to resources & tools

QUESTIONS?

RESOURCES

- http://www.windowsecurity.com/articles/Windows-Server-2008-Firewall-Advanced-Security-Part1.html
- http://technet.microsoft.com/en-us/library/intro-wfas-ipsec(WS.10).aspx
- http://itsecurity.uiowa.edu

THANK YOU!

security@uiowa.edu