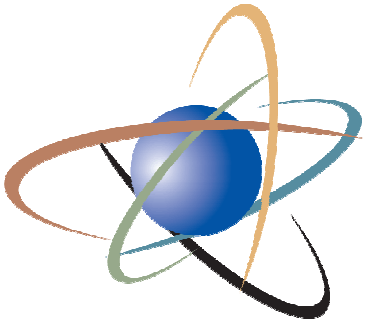


U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Firewall Presentation

Mike Shinn

Casey Priester

Disclaimer

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

This presentation:

- does not contain NRC official positions
- is not guidance on how to configure firewalls
- is an overview of firewalls and their limitations
- is a demonstration of how attackers can bypass firewalls

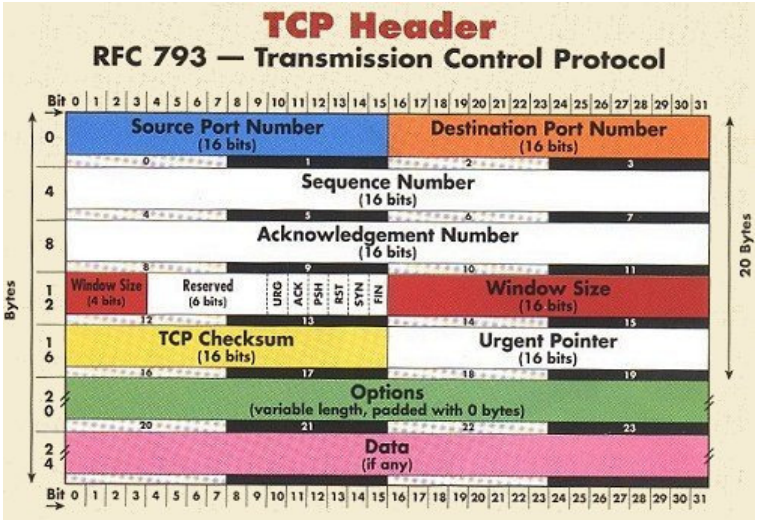
What is a Firewall?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Q: What is a firewall?

A: A firewall is a computer.

- A firewall has the following:
  - Two or more network cards
  - Processor, RAM, hard drive
  - Operating System



Q: What makes a firewall different from other computers?

A: Very little.

- Designed to analyze and filter data flows at its most basic level
- May include additional logic to perform real-time contextual analysis of data flows
- May include specialized networking hardware to aid in this task

What is a Firewall?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Q: What is the purpose of a firewall?

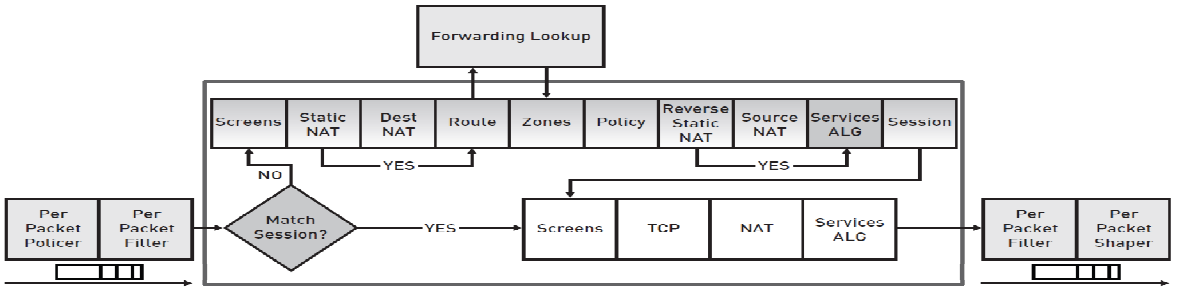
A: To control the flow of data between networks according to pre-defined rules

- Packet Filtering (by port, by protocol, by source address, by destination address)
- Stateful Inspection (can determine if a packet is part of an existing data flow)
- Other features include the following:

  -"Application Aware:" contains logic specific to common application (web, FTP, Secure Shell, etc.)

  - Quality of Service: Traffic prioritization and scheduling

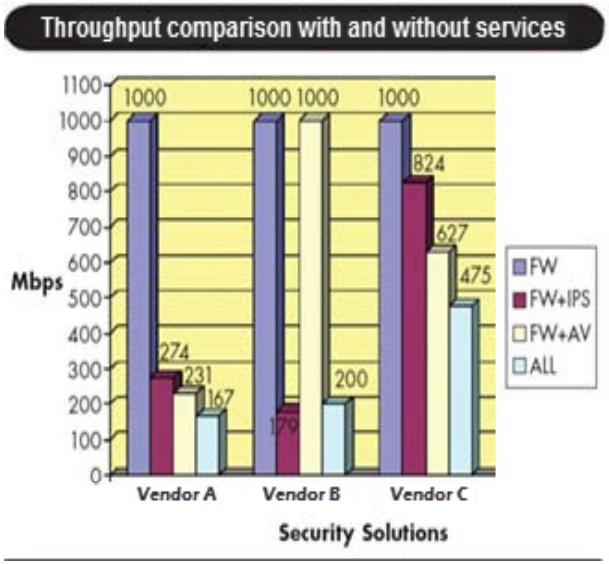
  - Session Inspection: Can search a data flow for certain types of content



Firewall Limitations

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- A firewall cannot perform all security tasks
  - Hardware limitations
  - Memory and overhead limitations
  - Time limitations
  - Logic limitations
  - Encrypted traffic payloads are not visible
  - Firewalls do not typically do traffic normalization



- As a computer, a firewall can have vulnerabilities
  - CVE-2012-4661: Multiple Vulnerabilities in Cisco ASA 5500 Series Adaptive Security Appliances and Cisco Catalyst 6500 Series ASA Services Module
  - CVE-2012-5316: Multiple cross-site scripting (XSS) vulnerabilities in Barracuda Spam & Virus Firewall 600
  - **ICSA-12-102-05: Siemens Scalance S Multiple Security Vulnerabilities**

Firewall Limitations

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

A firewall is only as good as its ruleset.

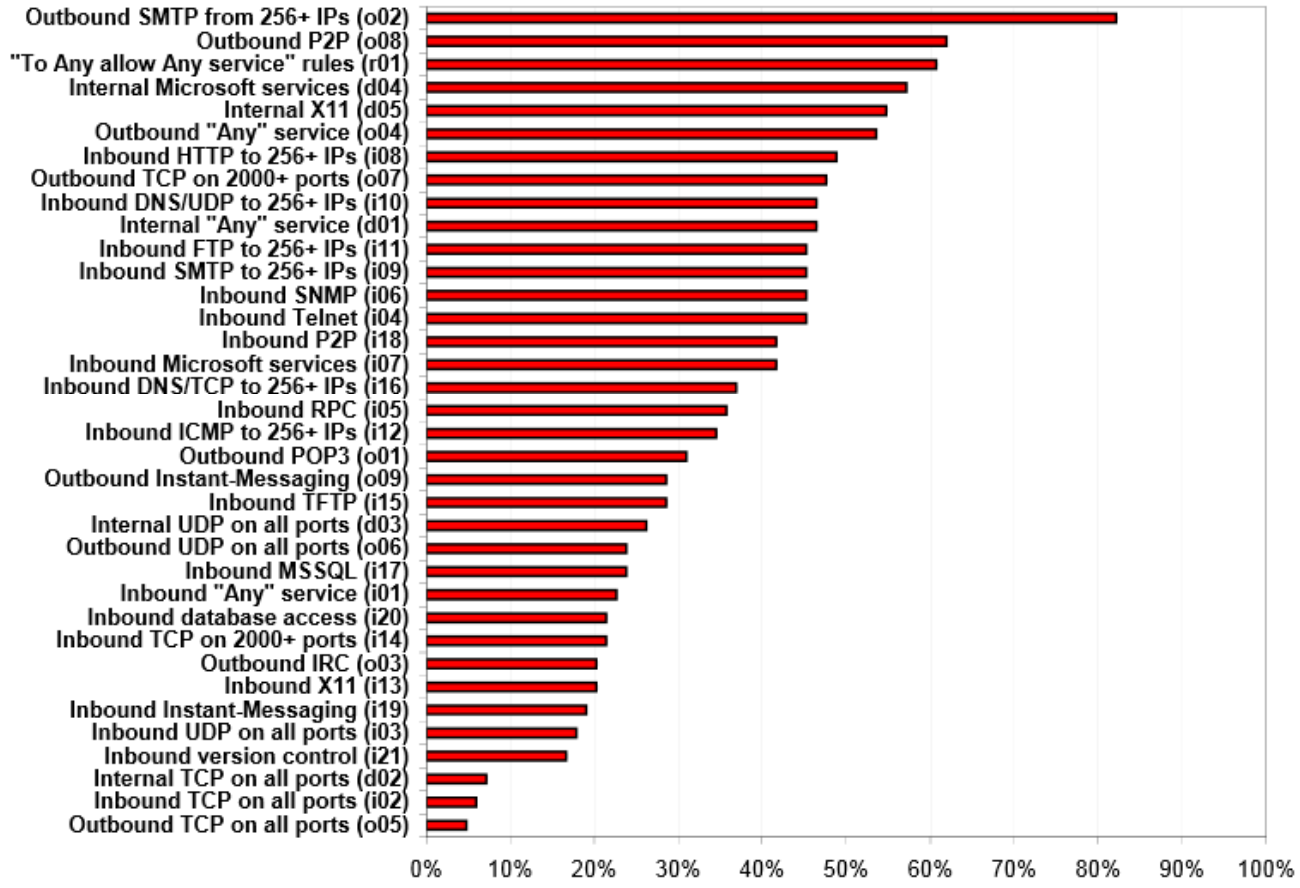


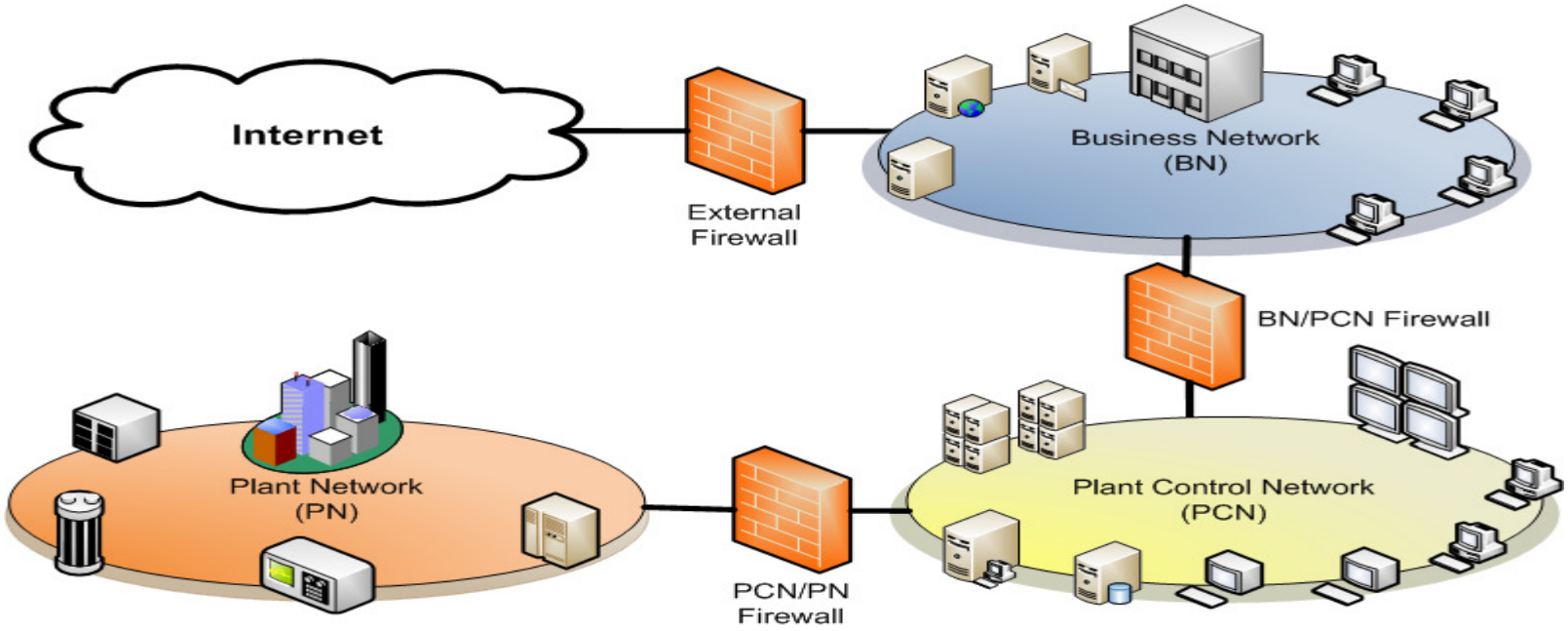
Figure 2: Distribution of configuration errors.

Source: Wool, Avishai. (2009). Firewall configuration errors revisited. Tel Aviv University School of Engineering. Retrieved from: http://arxiv.org/pdf/0911.1240v1.pdf

Typical Network Architecture

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Business network acts as backbone
- Firewall between business network (BN) and plant control network (PCN)
- Firewall between PCN and plant network (PN) may or may not be in place

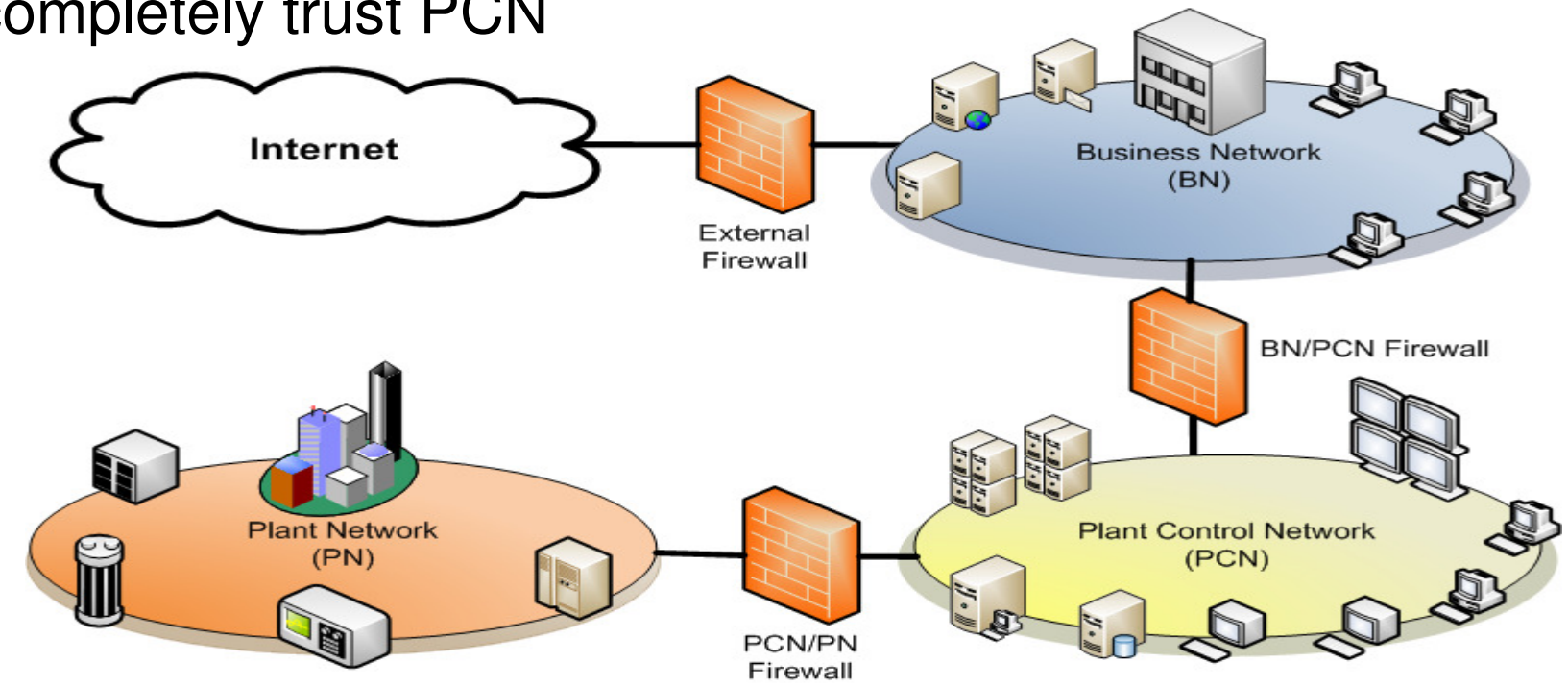


Typical Network Architecture

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Problems:

- BN/PCN Firewall is configured to partially or completely trust BN
- PCN/PN Firewall is configured to partially or completely trust PCN



Common Weaknesses to Model

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Poorly configured firewalls (historical, political, or legacy technical reasons)
  - Passing Microsoft Windows networking packets
  - Passing remote services (rsh, rlogin)
  - PCN/PN having trusted hosts on the business LAN
  - Not providing outbound data rules

- Peer links that bypass or route through external firewall direct to PCN or PN

Common Weaknesses to Model

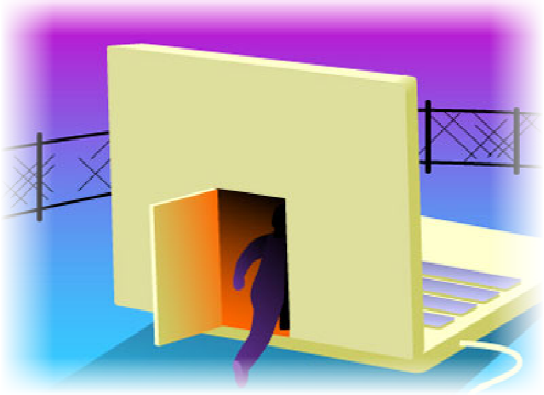
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- IT controlled assets in the PCN or PN (communications links, replicated services)
- Vendor links for remote maintenance/monitoring
- Out-of-band communications channels (backup links to RTUs)

Getting Inside the Trusted Network

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Passive Evasion - The victim "phones home" to the attacker
  1. Phishing/spearphishing
  2. Malicious website/drive-by infection
  3. "Sneakernet" infection
  4. Social Engineering



- Indirect Evasion – Traffic appears to be authentic
  1. Stolen remote access credentials
  2. VPN piggyback
  3. Session hijacking
  4. Address spoofing (for internal zones)

Getting Inside the Trusted Network

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Active Evasion
  1. Attack exposed services (Web, E-mail)
  2. Attack firewall vulnerabilites
  3. Exploit weak ruleset/poor configuration
  4. “Trick” or subvert the firewall logic with protocol manipulation (AET)
  5. Find out-of-band channels (wireless, modems, satellite links)
  6. Get physical access to firewall or other infrastructure

Case Study – Palo Alto Networks

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Founded in 2005 by Checkpoint veteran
- First firewall product developed in 2007
- First of the "Next Generation" firewalls1
- Named leader in the 2011 Gartner "Magic Quadrant" report2
- At Defcon 19 (Dec 2011), Palo Alto firewall demonstrated to have fatal design flaw

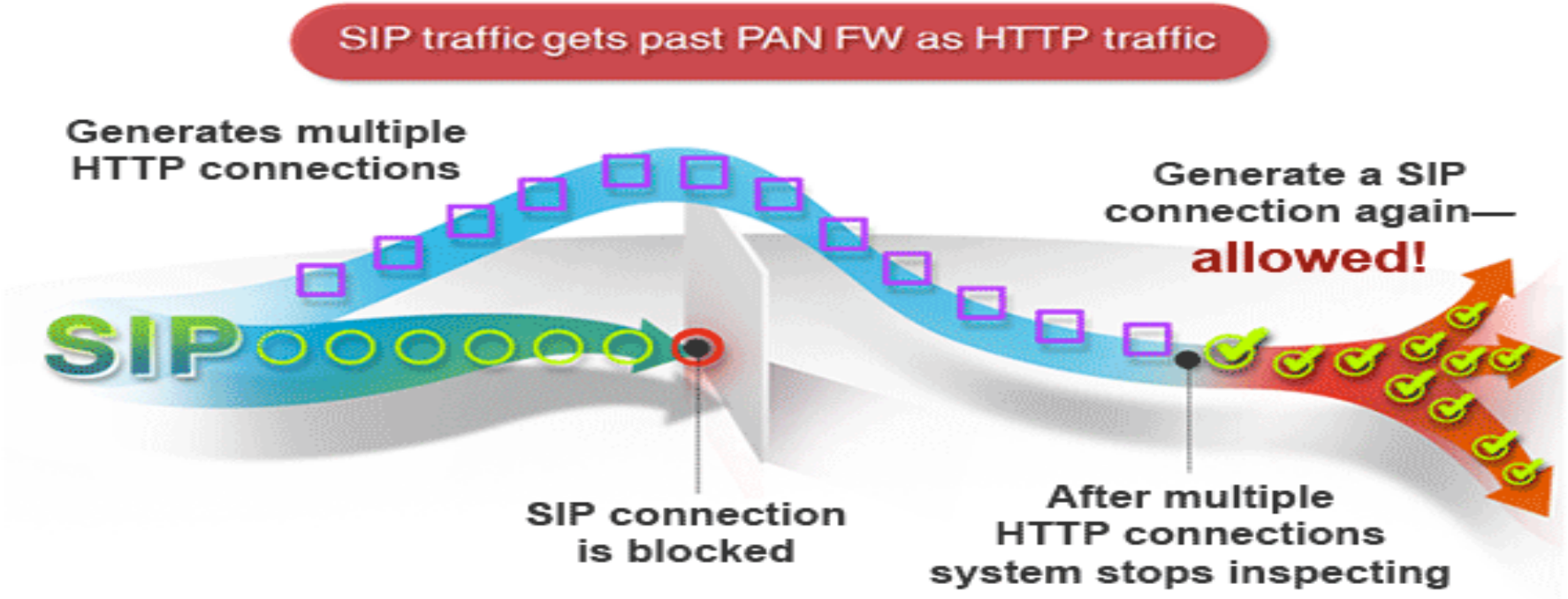
1. Pescatore, J. & Young, G. (2009, October 19). Defining the Next-Generation Firewall. Gartner RAS Core Research Group. Retrieved from: http://img1.custompublish.com/getfile.php/1434855.1861.sqqycbrdwq/Defining+the+Next-Generation+Firewall.pdf, retrieved 2012-12-02
2. Denne, S. (2011, December 16). Palo Alto Networks hits the Magic Quadrant for firewalls. The Wall Street Journal. Retrieved from: http://blogs.wsj.com/venturecapital/2011/12/16/palo-alto-networks-hits-the-magic-quadrant-for-firewalls/
3. Woodberg, B. (2011). Palo Alto Networks Security Bypass. Defcon 19. Retrieved from: http://www.youtube.com/watch?v=AuaCrRIlgnQ

Case Study – Palo Alto Networks

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Cache poisoning attack:

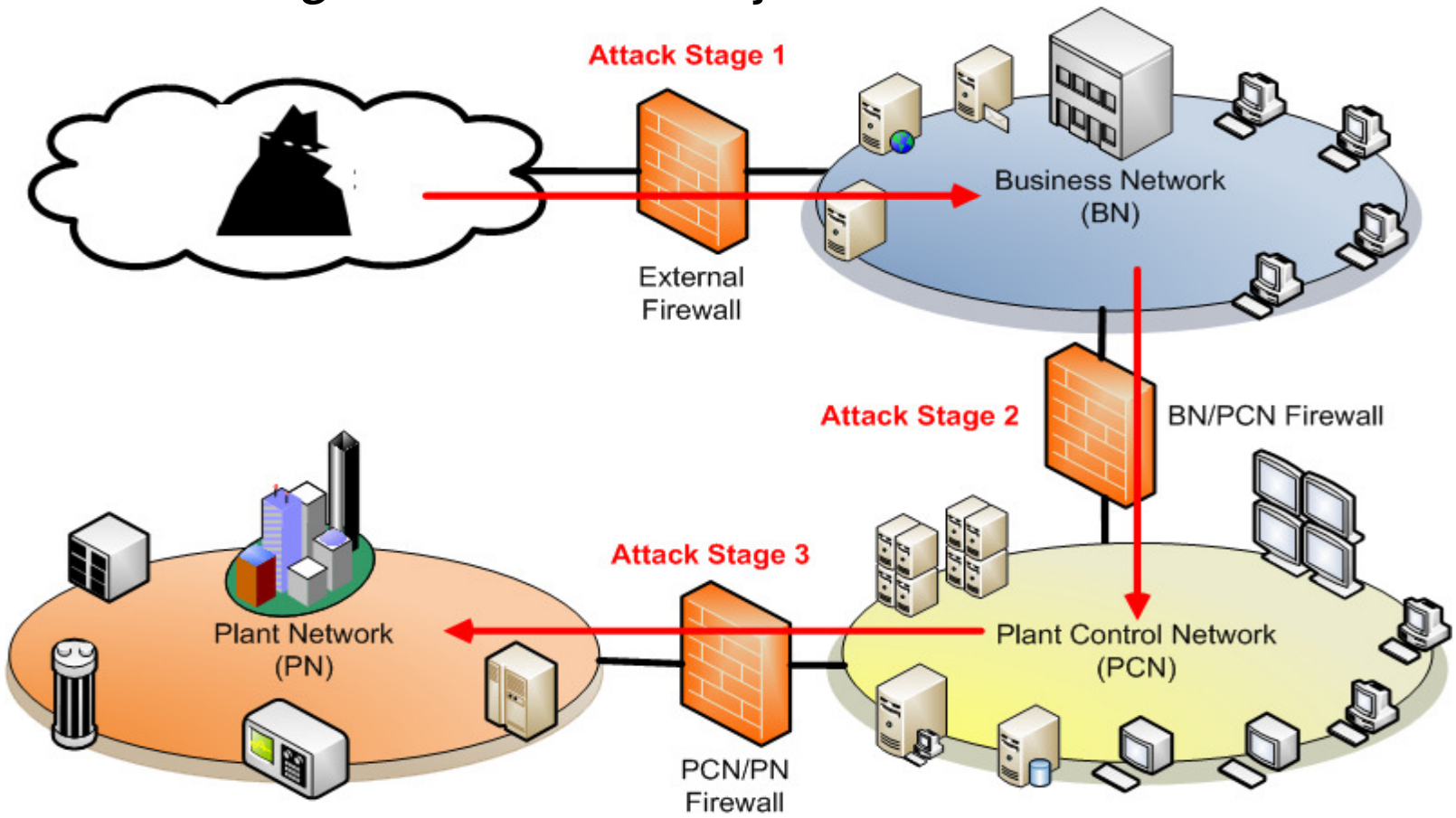
- HTTP port open, SIP port blocked
- Attacker generates large number of HTTP sessions
- Memory cache fills, traffic no longer inspected
- HTTP session re-established as SIP, bypassing filter



Demonstration

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Attack Stage 1 – Desktop attack
Attack Stage 2 – Impersonation Attack
Attack Stage 3 – Session Hijack



Attack Stage 1– Desktop Attack

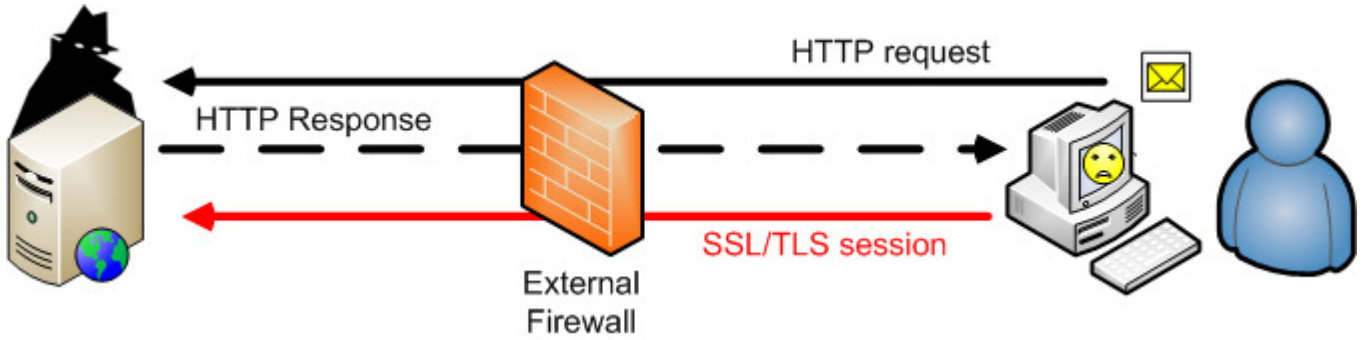
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Scenario 1:

- Attacker crafts email message to employee
  - Looks very believable, may come from spoofed address of trusted source
- Email contains link to compromised website

Scenario 2:

- Employee goes to trusted website, which has link to infected website, employees computer is infected without knowledge (watering hole attack)



Attack Stage 1– Desktop Attack

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Both Scenarios:

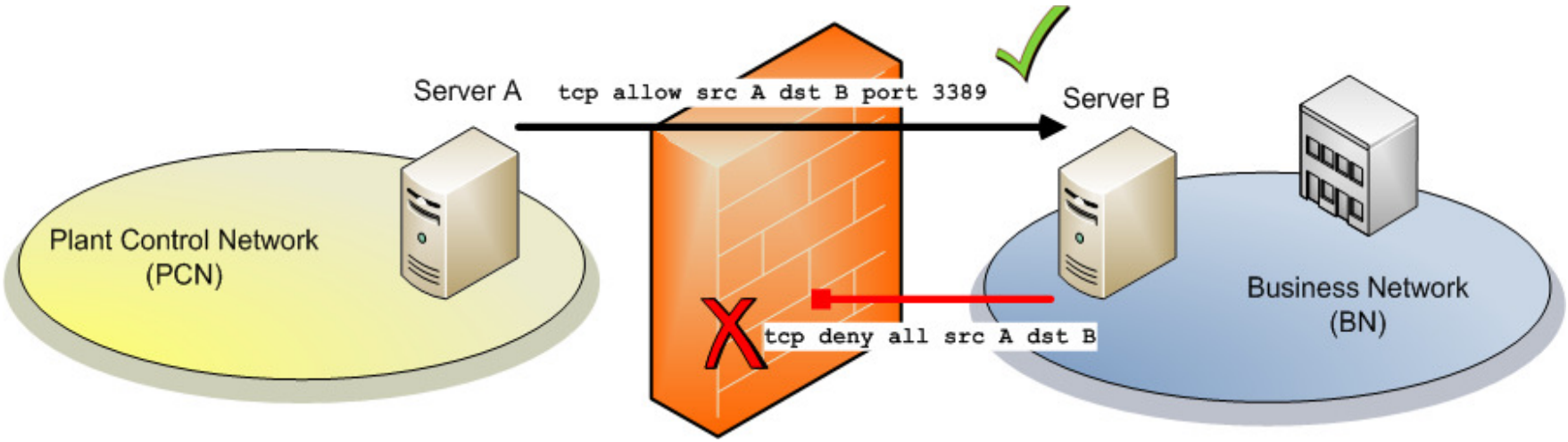
- Zero-day exploits in desktop software (e.g. browsers, operating system, browser plugin)
- Anti-virus/anti-malware measures will not detect if no signature available
- IDS/IPS will not detect if no signature available or if connection is encrypted
- Payload deploys rootkit or Remote Access Toolkit (RAT)
- Payload initiates outbound connection over SSL/TLS or other encrypted protocol to bypass IDS/IPS/firewall inspection measures
- Attacker now has full control over employee's system and can attack local servers

Attack Stage 2 – Impersonation Attack

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

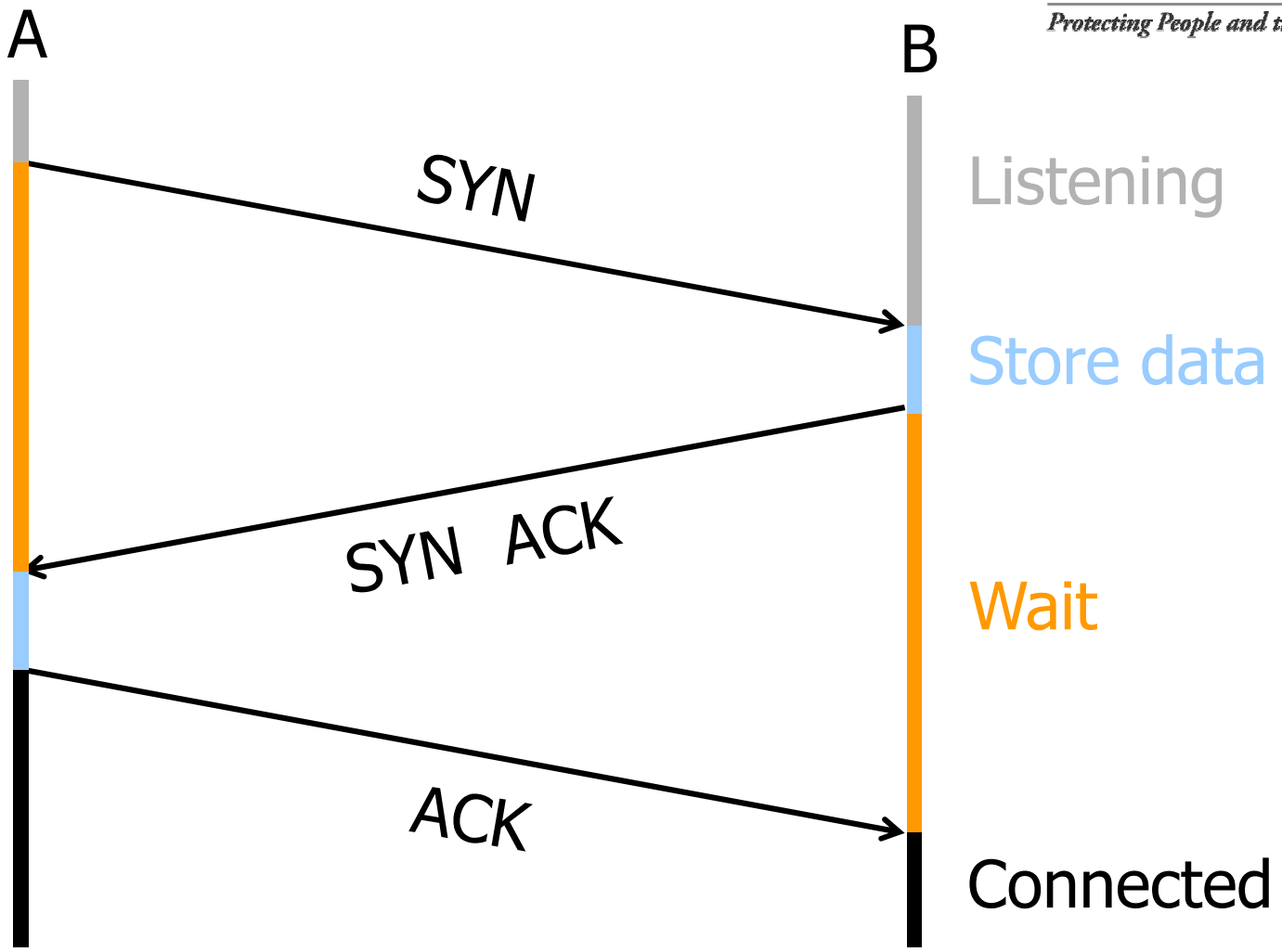
Scenario:

- No connections are allowed thru firewall from PCN to BN
- Firewall is configured as “one way”
- Server A, behind the firewall, sends a requests for data to Server B
- Server B cannot talk to Server A



TCP “Handshake”

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

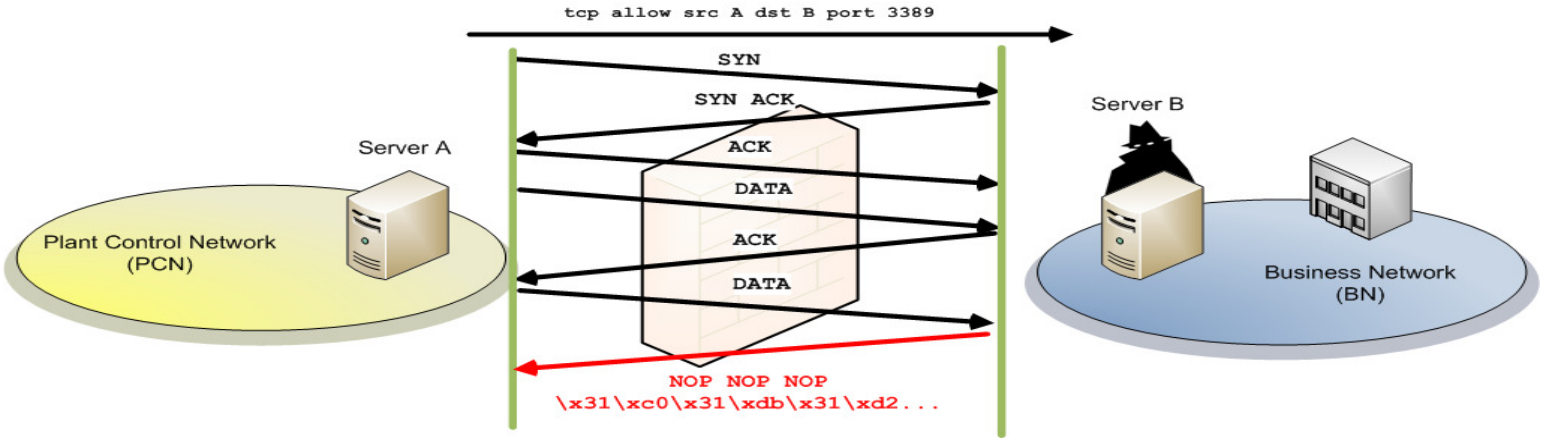


Once established, all TCP connections are bi-directional. Attacks can flow back to clients!

Attack Stage 2 Buffer Overflow

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- A buffer overflow occurs when attacker sends data that cannot be adequately handled by the victim program
  - -Unexpected value
  - -Value out-of-bounds
  - -Memory violation
- Attack packet contains executable instructions to request victim open a shell prompt
- The original session has **not** terminated

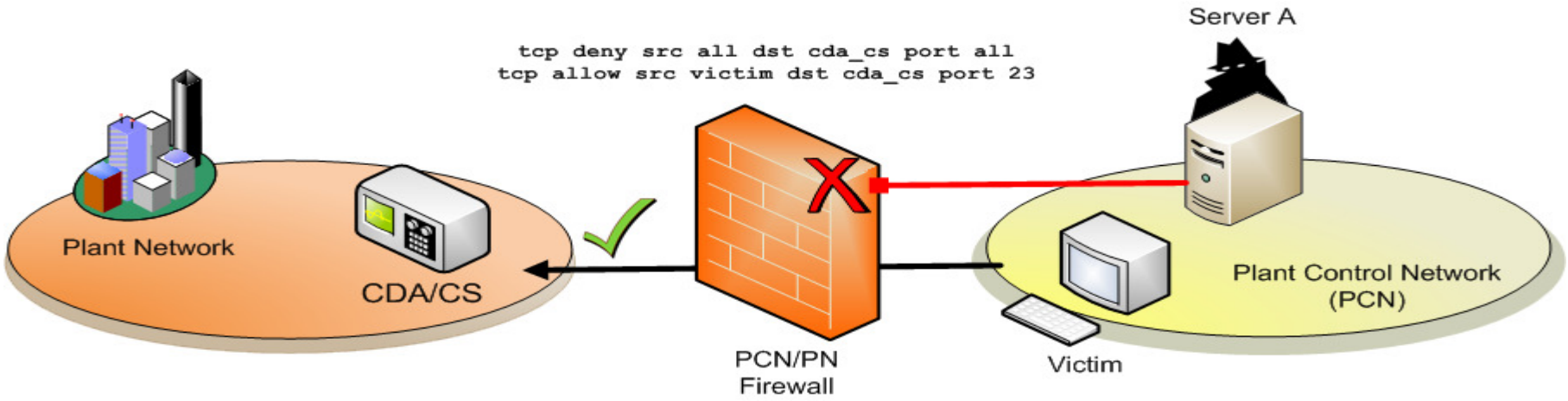


Attack Stage 3 – Session Hijack

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

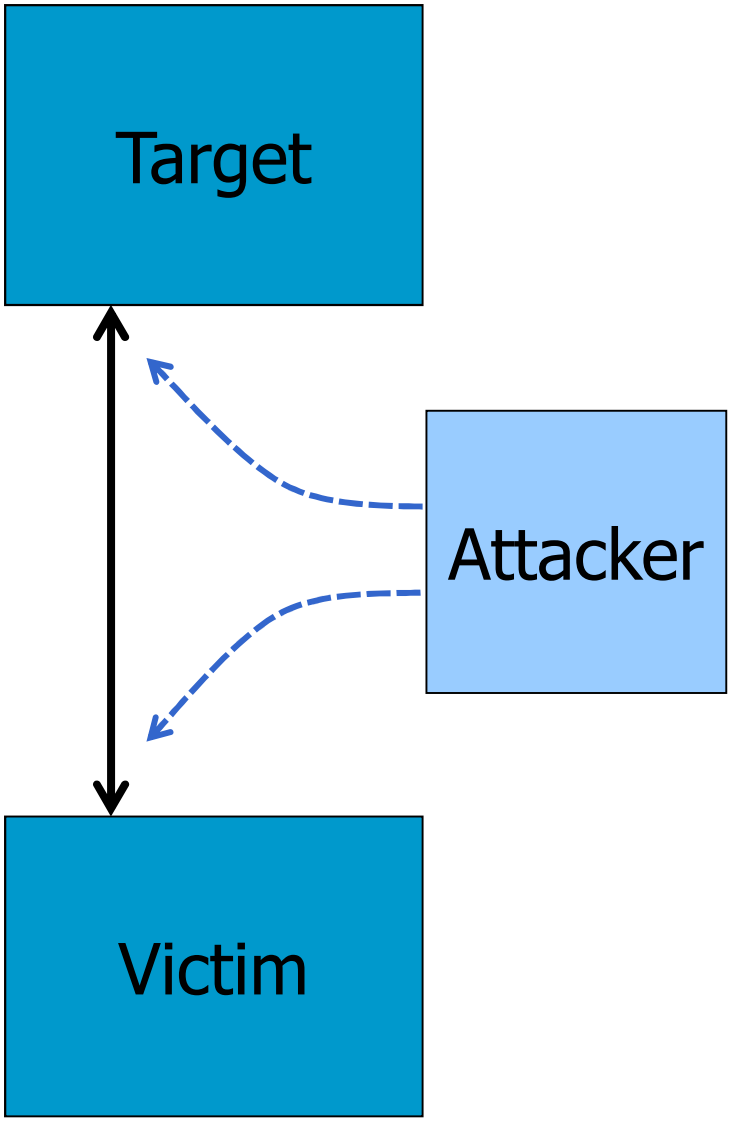
Scenario:

- Victim is logged into CDA/CS, through the firewall
- Telnet connection is allowed from Victim to ICS
- No other hosts are allowed to connect thru firewall to ICS
- Telnet Connection is authenticated



Blind TCP Session Hijacking

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

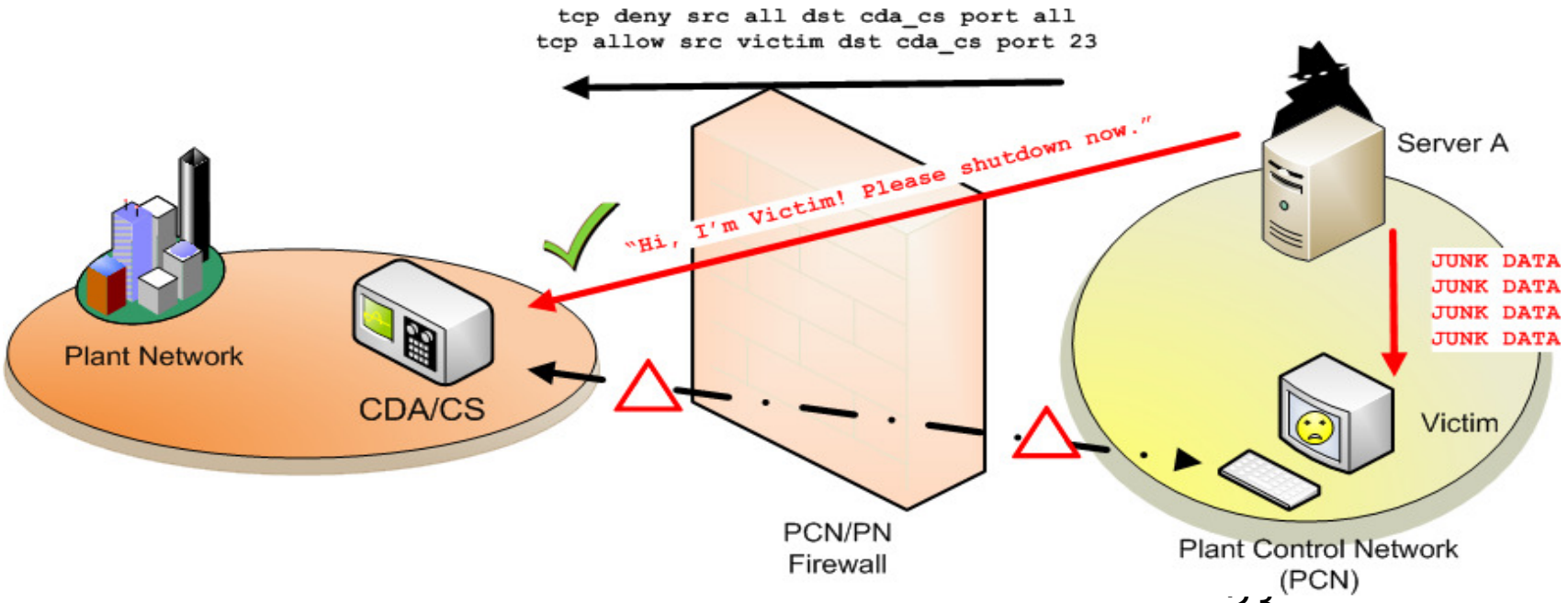


- Victim, target trusted authenticated connection
  - Packets will have predictable sequence numbers
- Attacker impersonates victim to target
  - Opens connection to target to get initial seq number
  - Fills victim's receive queue
  - Sends packets to target that resemble victim's transmission
  - Attacker cannot receive, but may execute commands on target

Attack Stage 3 – Session Hijack

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Attacker listens to unencrypted session
- Attacker uses probes to determine sequence numbers
- Attacker sends spoofed identity packets to ICS while performing Denial of Service on Victim
- Attacker sends shutdown command to ICS



How Easy are These Attacks?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Numerous RAT/trojan toolkits available on underground market
  - Push-button ease of use
  - Exploits as a Service (EaaS) becoming viable business model1,2
- Buffer overflow attack methodologies have been well-known and well-documented for many years
  - "Smashing the Stack for Fun and Profit" by AlephOne, *Phrack* magazine,1996
- Session hijacking is one of the oldest attack methods on the Internet
  - Kevin Mitnick "man-in-the-middle" attack, 1994

1. Grier, Ballard, Caballero, et. al. (2012). Manufacturing Compromise: The Emergence of Exploit-as-a-Service. 19th ACM Conference on Computer and Communications Security. Retrieved from http://cseweb.ucsd.edu/~voelker/pubs/eaas-ccs12.pdf
2. Asprey, D. (2011). New type of cloud emerges: Exploits as a Service (EaaS). TrendMicro Security. Retrieved from http://cloud.trendmicro.com/new-type-of-cloud-emerges-exploits-as-a-service-eaas/

How Easy are These Attacks?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Free, easily available hacking tools and toolkits can perform some or all firewall bypass attack types:
  - -Metaploit Framework
  - -Cain and Abel
  - -Firesheep
  - -LOIC
  - -Evader
  - -Backtrack Live CD
  - -Nmap
  - -Ettercap

Firewall Limitations

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Firewall technology is not one way (non-deterministic, not application-fluent)
- Firewalls can be bypassed in many ways
- Firewalls have their own vulnerabilities
- Effective Security Programs must do the following:
  - -Prevent
  - -Detect
  - -Delay
  - -Deny
  - -Deter
  - -Respond
  - -Recover
- Firewalls cannot do all of these things alone