13 Ways Through A Firewall
What you don’t know will hurt you

Andrew Ginter
Director of Industrial Security
Waterfall Security Solutions
Firewalls

- Firewalls – separate networks and sub-networks with different security / connectivity needs
- Often first investment any site makes when starting down the road to an ICS cyber security program
- “Unified Threat Managers” – firewalls with stateful inspection, VPNs, in-line anti-virus scanning, intrusion detection, intrusion prevention, anti-spam, web filtering, and much more – but are they secure?
- DMZ – “in-between” network(s)
- ICS best practice: layers of firewalls, layers of host and network-based defenses

Photo: Red Tiger Security
Setup for Demo Scenarios

- Industrial firewall / UTM
- Business network – my laptop + “hacked host” virtual machine
- Control network – ICS server to attack / take over + one other ICS host virtual machine
- 2x virtual switches – one for each network, each connected to firewall
- Consider only one-hop compromise – into DMZ, or into ICS from DMZ
## Compensating Measures

<table>
<thead>
<tr>
<th>Abbrev</th>
<th>Compensating Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-FACT</td>
<td>2-Factor authentication</td>
</tr>
<tr>
<td>ENC</td>
<td>Encryption</td>
</tr>
<tr>
<td>RULES</td>
<td>Better firewall rules</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host intrusion detection / prevention system / SIEM</td>
</tr>
<tr>
<td>NIDS</td>
<td>Network intrusion detection / prevention system / SIEM</td>
</tr>
<tr>
<td>SECUPD</td>
<td>Security updates / patch program</td>
</tr>
<tr>
<td>UGW</td>
<td>Unidirectional security gateway</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Graphic</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Would have prevented / detected the attack</td>
</tr>
<tr>
<td>Yellow</td>
<td>Would prevent / detect some variants of the attack</td>
</tr>
<tr>
<td>Red</td>
<td>Would not have prevented / detected the attack</td>
</tr>
</tbody>
</table>
#1 Phishing / Spam / Drive-By-Download

- Single most common way through (enterprise) firewalls
- Client on business network pulls malware from internet, or activates malware in email attachment
- “Spear-phishing” – carefully crafted email to fool even security experts into opening attachment
#2 Social Engineering – Steal a Password

- VPN password on sticky note on monitor, or under keyboard
- Call up administrator, weave a convincing tale of woe, and ask for the password
- Ask the administrator to give you a VPN account
- Shoulder-surf while administrator enters firewall password
- Guess
- Install a keystroke logger
#3 Compromise Domain Controller – Create Account

- More generally – abuse trust of external system
- Create account / change password of exposed ICS server, or firewall itself
- Other external trust abuse – compromise external HMI, ERP, DCS vendor with remote access, WSUS server, DNS server, etc.
#4 Attack Exposed Servers

- Every exposed port is vulnerable:
  - SQL injection
  - buffer overflow
  - default passwords
  - hard-coded password
  - denial of service / SYN-flood
#5 Attack ICS Clients via Compromised Servers

- Best practice: originate all cross-firewall TCP connections on ICS / trusted side
- Once established, all TCP connections are bi-directional – attacks can flow back to clients:
  - compromised web servers
  - compromised files on file servers
  - buffer overflows
#6 Session Hijacking / Man-in-the-Middle

- Requires access to communications stream between authorized endpoints – eg: ARPSpoof (LAN), fake Wi-Fi access point, hacked DNS server
- Insert new commands into existing communications session
- Sniff / fake session ID / cookie and re-use
#7 Piggy-Back on VPN

- You may trust the person you have granted remote access, but should you trust their computer?
- Broad VPN access rules – “I trust this user to connect to any machine, on any port” makes it easy for worms and viruses to jump
- Split-tunneling allows interactive remote control
#8 Firewall Vulnerabilities

- Firewalls are software. All large software artifacts have bugs, and some of those bugs are security vulnerabilities and zero-days
- Vendor back-doors / hard-coded passwords
- Supply chain issues – do you trust the manufacturer? The manufacturer’s suppliers?
- Occasional design vulnerabilities
#9 Errors and Omissions

- Modern firewalls require 6-8 weeks full-time training to cover all features and all configurations
- The smallest errors expose protected servers to attack
- Over time, poorly-managed firewalls increasingly resemble routers
- Well-meaning corporate IT personnel often control firewall configurations and can reach through to “fix” ICS hosts
#10 Forge an IP Address

- Most firewall rules are expressed in terms of IP addresses.
- Any administrator can change the IP address on a laptop or workstation.
- Works only if attacker is on the same LAN segment as the true IP address— or WAN routers route response traffic to a different LAN.
- May need ARPspoof to block the machine with the real IP.
#11 Bypass Network Security Perimeter

- Complex network architectures – path from business network to ICS network through only routers exists, but is not obvious
- Rogue wireless access points
- Rogue cables – well meaning technicians eliminate “single point of failure” in firewall
- ICS network extends outside of physical security perimeter
- Dial-up port
#12 Physical Access to Firewall

- If you can touch it, you can compromise it
- Reset to factory defaults
- Log in to local serial port, change settings with CLI
- Re-arrange wiring
#13 Sneakernet

- Removable media, especially USB sticks, carried past physical / cyber security perimeter
- Entire laptops, workstations and servers carried past physical / cyber security perimeter
Demo

Warning: the issues demonstrated in the following slides apply to all firewalls, not just the firewall vendors and models illustrated. It is a mistake to interpret the following slides as a criticism of specific firewalls or specific firewall vendors.
# Keeping Score

<table>
<thead>
<tr>
<th>Graphic</th>
<th>Score</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>Would have prevented / detected the attack</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Would prevent / detect some variants of the attack</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Would not have prevented / detected the attack</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Score</th>
<th>Abbrev</th>
<th>Compensating Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-FACT</td>
<td>7</td>
<td>2-Factor authentication</td>
</tr>
<tr>
<td>ENC</td>
<td>7</td>
<td>Encryption</td>
</tr>
<tr>
<td>RULES</td>
<td>11</td>
<td>Better firewall rules</td>
</tr>
<tr>
<td>HIDS</td>
<td>8</td>
<td>Host intrusion detection / prevention system / SIEM</td>
</tr>
<tr>
<td>NIDS</td>
<td>9</td>
<td>Network intrusion detection / prevention system / SIEM</td>
</tr>
<tr>
<td>SECUPD</td>
<td>9</td>
<td>Security updates / patch program</td>
</tr>
<tr>
<td>UGW</td>
<td>20</td>
<td>Unidirectional security gateway</td>
</tr>
</tbody>
</table>
Waterfall Security Solutions

- Headquarters in Israel, sales and operations office in the USA
- Hundreds of sites deployed in all critical infrastructure sectors
- Frost & Sullivan: Entrepreneurial Company of the Year Award for ICS network security
- Pike Research: Waterfall is key player in the cyber security market
- Gartner: IT and OT security architects should consider Waterfall for their operations networks
- Strategic partnership agreements / cooperation with: OSIsoft, GE, Siemens, and many other major industrial vendors

*Market leader for server replication in industrial environments*
Stronger Than Firewalls

- Firewalls are porous
- Given the “elephants in the room,” perimeter protection will always be disproportionately important:
  - 100,000 vulnerabilities
  - Plain-text device communications
  - Dissonance between ECC and IT’s “constant change” patch programs
  - Long life-cycles for physical equipment

Analyst advice: All ICS security professionals should become familiar with Unidirectional Security Gateways as an alternative to firewalls