FORTINET
Training Institute

FORTINET
CERTIFIED
SOLUTION
SPECIALIST
Security
Operations

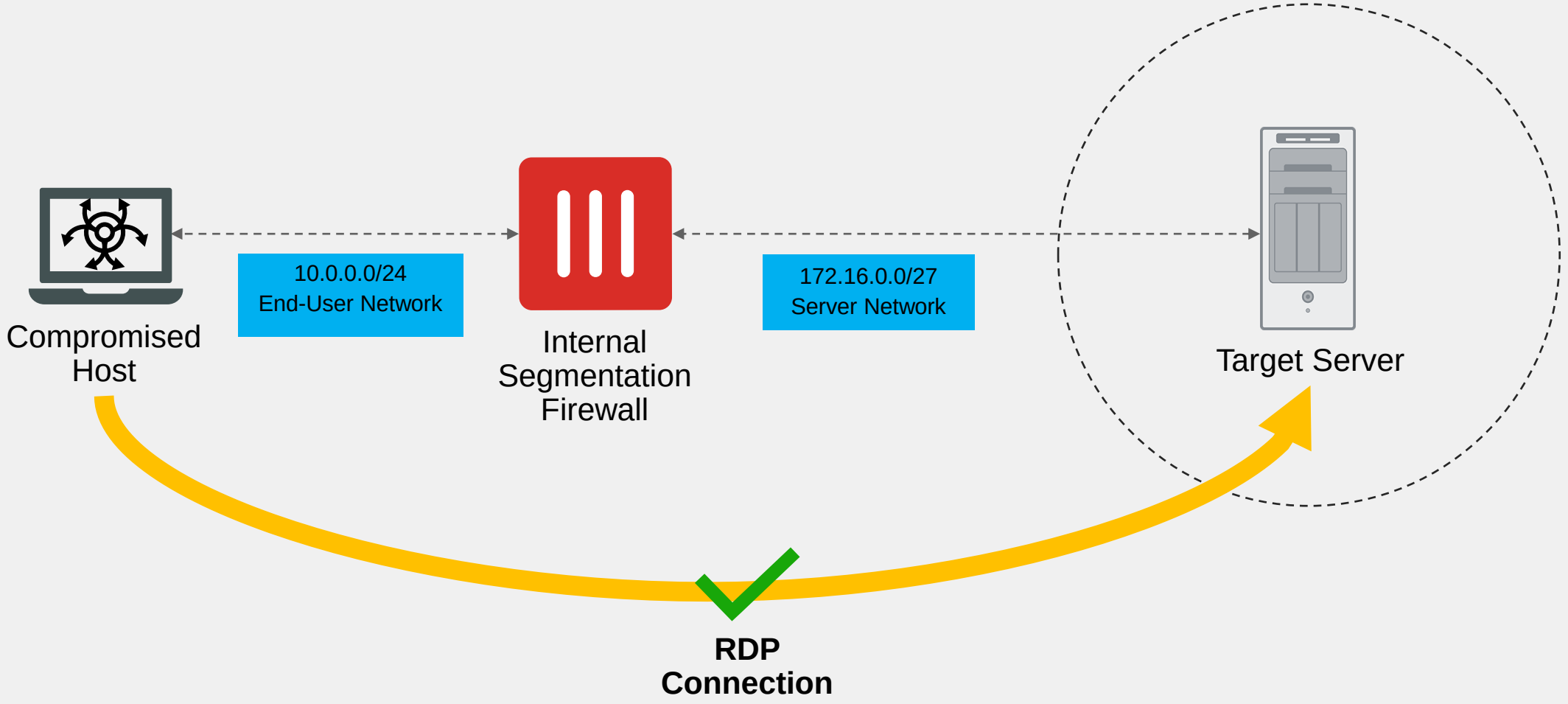
Security Operations Analyst

Attack Surface and Vectors

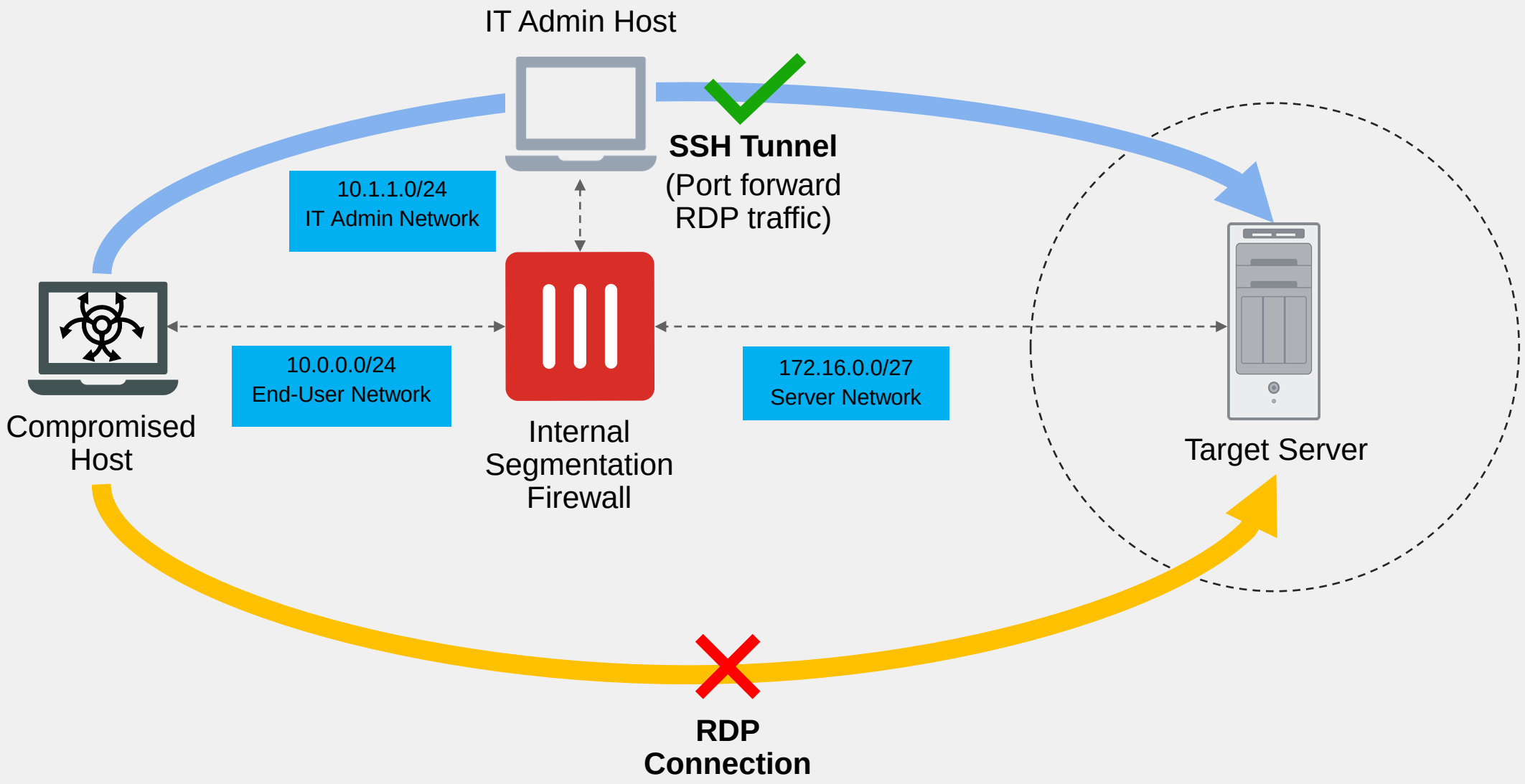
FortiAnalyzer 7.4

Last Modified: 22 January 2025

Lateral Movement



Lateral Movement (Contd)

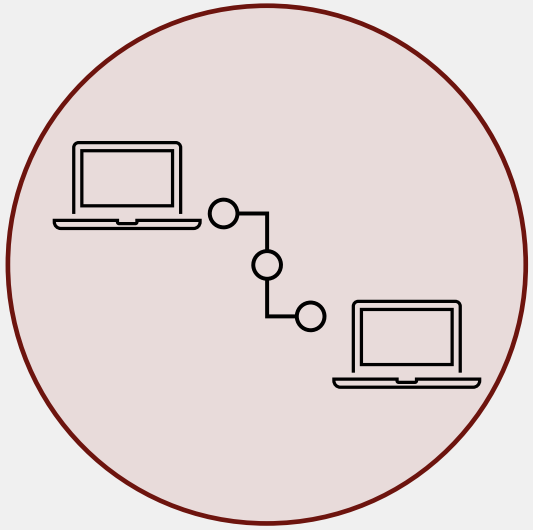


Restricting Lateral Movement

- Segment the network to reduce risk and exposure
- Implement zero trust network access
- Use multi-factor authentication for logins
- Keep approved accounts to a minimum
- Block network discovery mechanisms
- Monitor and log critical devices for suspicious logins and traffic flows
- Install software updates regularly

Persistence

- Used by attackers to maintain a connection with a compromised system
- Connection persists through reboots, log ins and log outs, and changed credentials
- Examples:
  - Modify registry keys to execute malicious programs during startup
  - Modify system services or create new services to run malicious programs
  - Modify logon scripts using Group Policy to execute malicious programs
  - Embed malicious macros in an office document
  - Place a malicious DLL in a location that makes an application run it



Defense Evasion

- Used by attackers to avoid detection after they initiate an attack

- Examples:
  - Encrypt malicious payloads to bypass security measures
  - Execute malicious actions directly in memory without leaving files
  - Modify file timestamps to confuse time-based analysis
  - Create malicious processes with system-like names

Review

- ✓Describe the attack surface
- ✓Describe how to identify the attack surface
- ✓Describe how to reduce the attack surface
- ✓Describe common attack vectors
- ✓Describe security best practices against attack vectors
- ✓Describe defenses against attack vectors
- ✓Describe how to capture traffic on Fortinet devices
- ✓Describe how to capture traffic on an endpoint
- ✓Describe how to use Wireshark to analyze packet captures