Northwest State Community College

Secure Remote ICS Access Using a VPN and Firewall

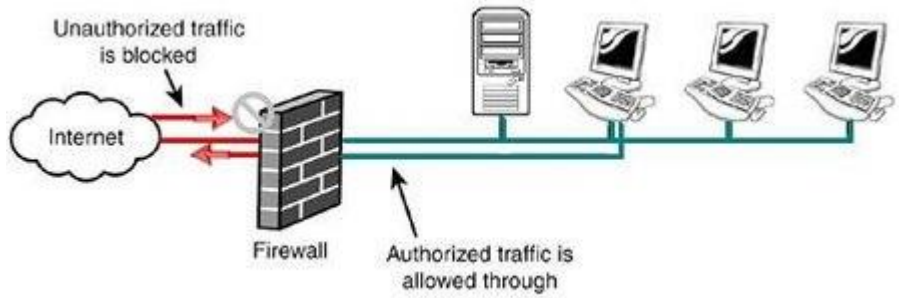
Made possible through support from the National Science Foundation (NSF) award number 1800929

Objectives

- Explain basic firewall concepts.
- Explain basic Virtual Private Network (VPN) concepts.
- Compare different VPN technologies.
- Demonstrate how the use of a firewall can prevent many remote attacks.
- Demonstrate how the use of VPN secures network traffic.

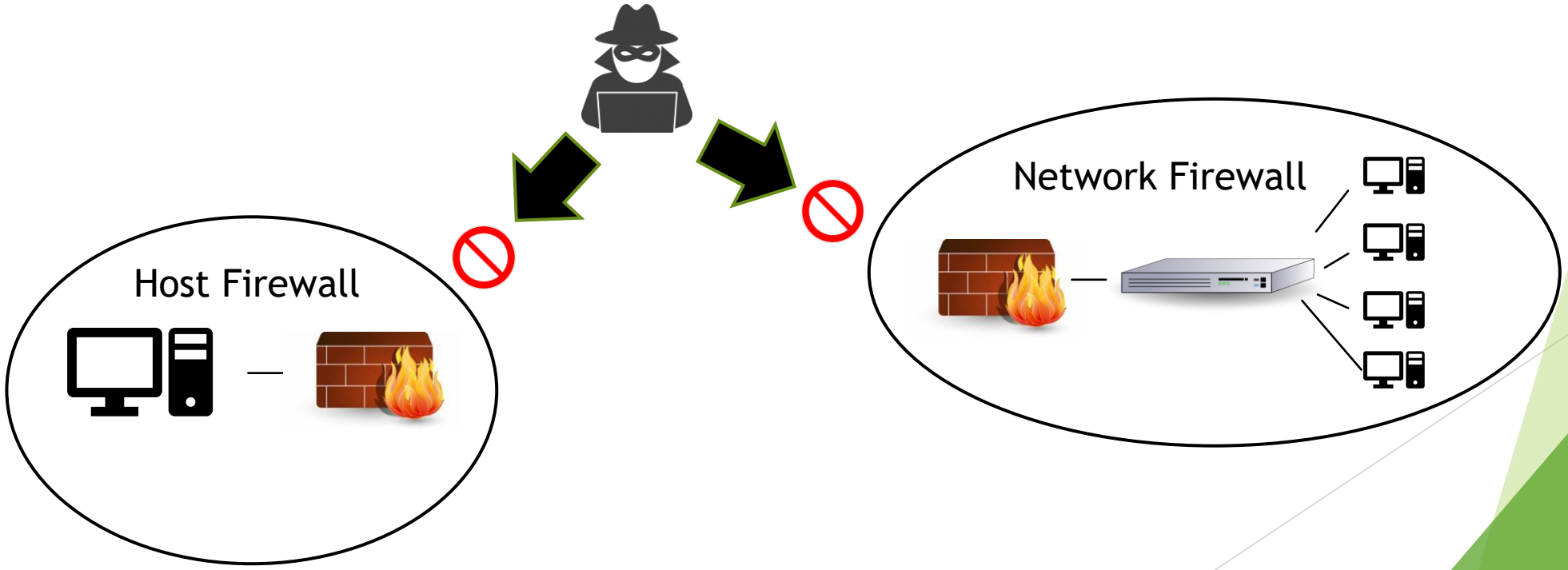
Firewall Basics

- The purpose of a firewall is to allow authorized traffic and prevent unauthorized traffic
  - Typically, outbound traffic is mostly unrestricted while inbound traffic is severely restricted



Firewall Basics

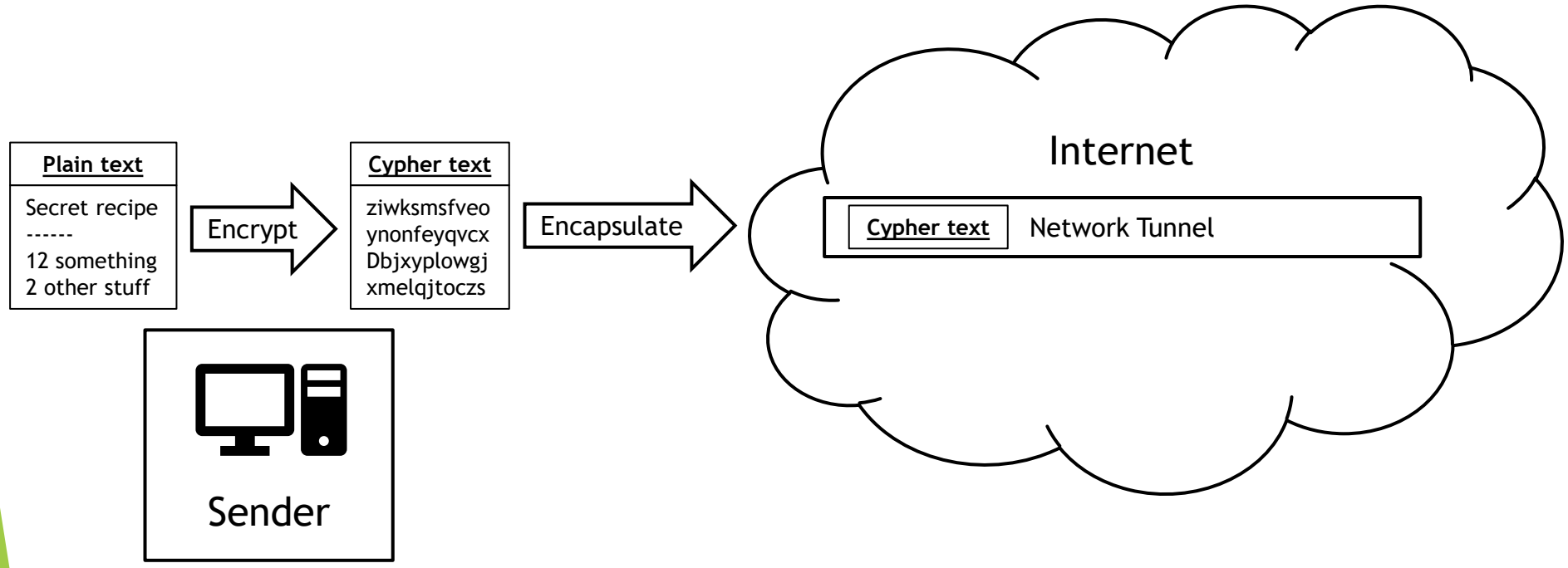
- Firewalls can be broadly classified into two categories
  - Host based firewalls protect a single host
  - Network based firewalls protect all systems on the same network segment



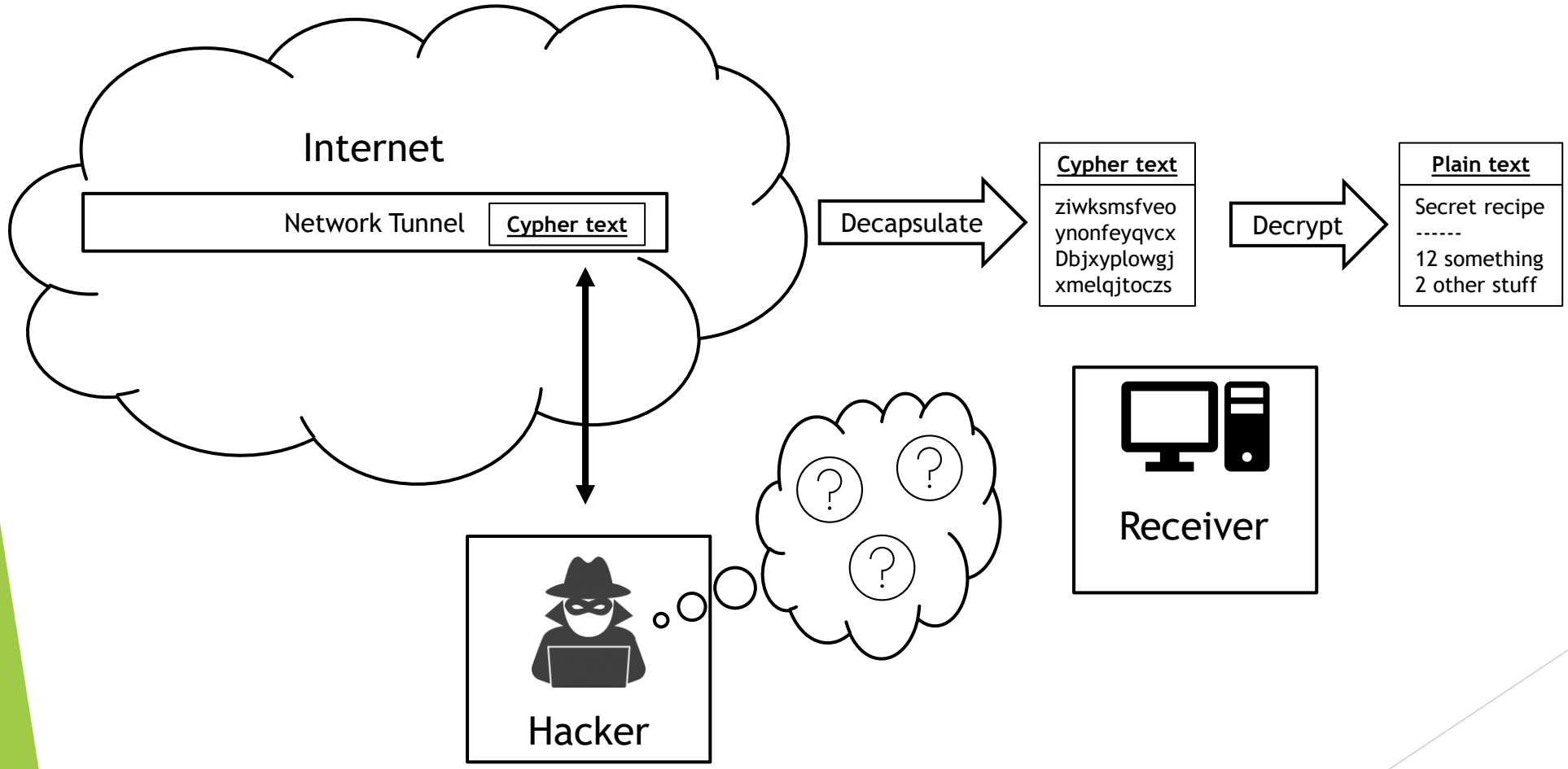
VPN Basics

- VPN – Virtual Private Network
  - Creates a private tunnel by encrypting data prior to sending it and decrypting the data when it is received

VPN Basics


Plain text
Secret recipe
---
12 something
2 other stuff
Encrypt
Cypher text
ziwksmsfveo
ynonfeyqvcx
Dbjxyplowgj
xmelqjtoczs
Encapsulate
Internet
Cypher text
Network Tunnel
Sender

VPN Basics


Internet
Network Tunnel
Cypher text
Decapsulate
Cypher text
ziwksmsfveo
ynonfeyqvcx
Dbjxyplowgj
xmelqjtoczs
Decrypt
Plain text
Secret recipe
------
12 something
2 other stuff
Receiver
Hacker

VPN Technologies

- PPTP - Point to Point Tunneling Protocol
  - Simple to setup
  - Not secure
- L2TP – Layer 2 Tunneling Protocol/IPSec – IP Security
  - L2TP – Provides basic unsecured tunneling
  - IPSec – Secures the data in the L2TP tunnel

VPN Technologies

- SSTP - Secure Socket Tunneling Protocol
  - Uses SSL/TLS over TCP port 443 which prevents many firewall issues
- OpenVPN
  - Open source VPN solution which is often implemented using Linux
- Other
  - Many other VPN solutions exist including commonly used proprietary solutions from vendors such as Cisco