Firewall and VPN

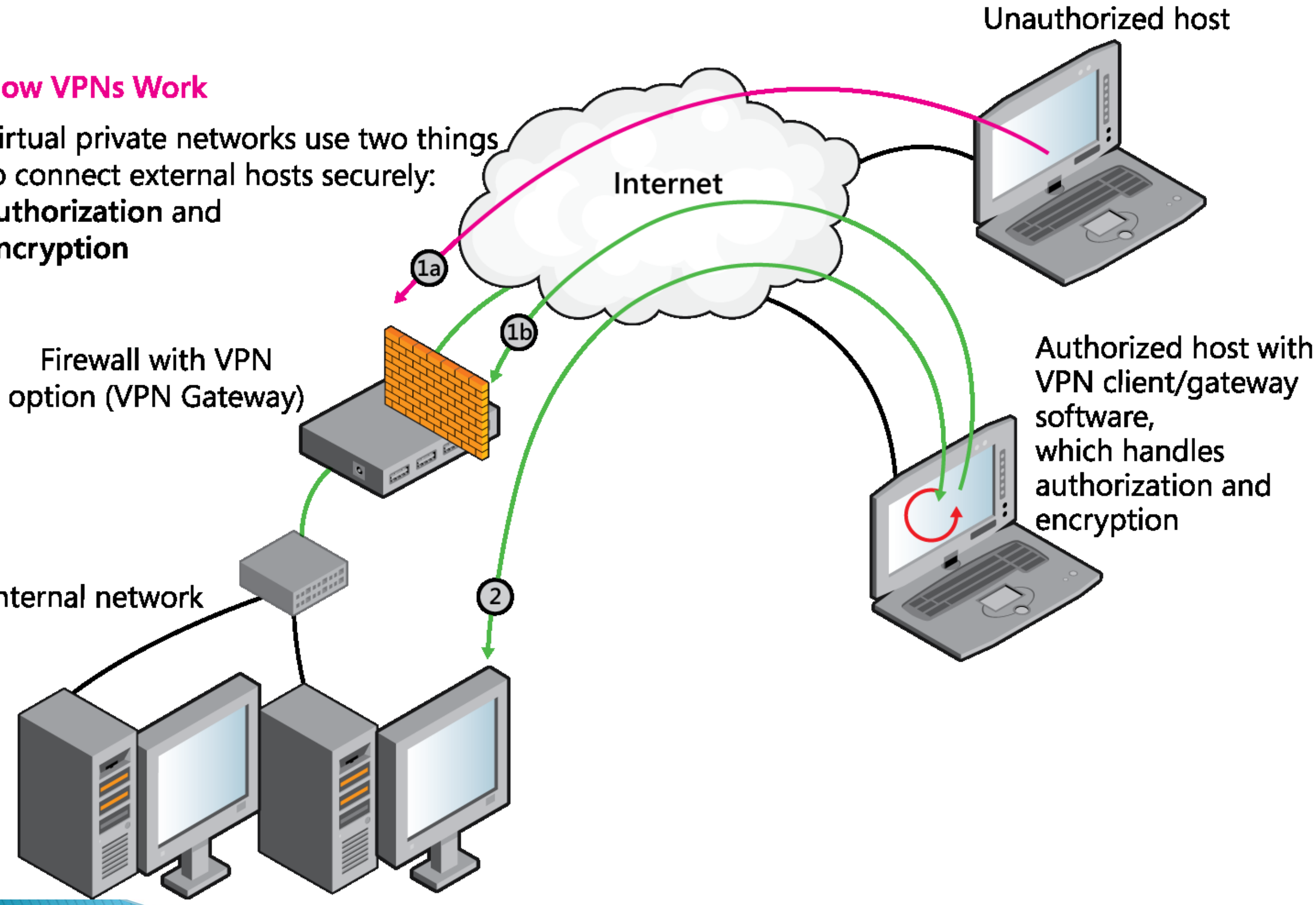
VPN

VPN

- Virtual private network are *nodes (*nodes are a connection point, either a redistribution point or a communication endpoint (some terminal equipment) on a public network
- They communicate among themselves using encryption so that their messages are safe from being intercepted by unauthorized users
- VPNs operate as if the nodes were connected by private lines. An example would be teachers at home needing limited access to the school district’s intranet would be given VPN software for their personal laptop

How VPNs Work

Virtual private networks use two things to connect external hosts securely: **authorization** and **encryption**


Unauthorized host
Internet
1a
1b
Firewall with VPN option (VPN Gateway)
Authorized host with VPN client/gateway software, which handles authorization and encryption
Internal network
2

Firewall

Firewall

- A computer system or network firewall is designed to permit authorized communications while blocking unauthorized access
- The device is configured to permit or deny computer applications based upon a set of rules and other criteria
- Firewalls are technological barriers designed to prevent unauthorized or unwanted communications between computer networks or hosts

Security Zone

Security Zone

- Business/organization's need for physical and logical boundaries for accessing, controlling, and securing information throughout an organization's network
- The security zone contains hidden settings for how Microsoft® Windows® and Internet Explorer® manage unsigned controls
- Security changes daily. A must to keep aware of the updates. Check the webcasts where leading security and privacy experts in field discuss the issues.
- Microsoft has webcasts covering Security Bulletins, Security Development Lifecycle, Security Intelligence Report, Security Tools, and more