Cyber CYA Series: IT and Security 101

Colorado SBDC
PIKES PEAK Small Business Development Center

Colorado SBDC TECHSOURCE
CYBER: Cover Your Assets™

CenturyLink®

www.pikespeaksbdc.org

Funded in part through a cooperative agreement with the U.S. Small Business Administration

Lamont Brooks

Sr Sales Engineer

Kyle McIntosh

CenturyLink/ Lead Sales Engineer

Security 101

CenturyLink

CenturyLink®

Our Mission Today

- Security Best Practices
- Firewall Types
- Open Forum to Answer All Your Questions

CenturyLink

Educate All Employees

Hackers don't break in, they log in

- The vast majority of breaches are the result of stolen passwords, not high-tech hacking tools.
- These break-ins are on the rise. Phishing scams, according to a recent FBI report. People lost more than **$57.8 million in 2019** as the result of phishing,
- As phishing becomes more profitable, hackers are becoming increasingly sophisticated in the methods.

CenturyLink

Use a True Firewall

Not all firewalls are the same

- Seems obvious but the firewall purchased at the big box store given to you by your provider doesn't always cut it.
- **Packet Filtering Firewalls**
- Firewalls that scan packet headers and compare them to Access Control Lists, or ACLs, set forth by a network security team are referred to as packet filters.
- The firewall takes apart the information located in the packet header such as IP address and port number to see if the packet is allowed/safe for the network.
- If the packet fails this firewall type's set criteria, it is dropped and unable to pass into the network.
- Packet filtering firewall are quick and convenient, but not foolproof.

CenturyLink

Firewall Types

Circuit-Level Gateway Firewalls

- 2Circuit-level gateway firewalls work similarly to their namesake – through the gateway.
- Allow requested information into the network, serving as a ‘gatekeeper’ of incoming information.
- They reroute the IP address of the workstation to that of the firewall, further protecting the network by hiding the IP address of all computers within that network.
- Close off ports that are not being requested for use by a user within the network.
- All incoming traffic that has not been requested by a user is immediately dropped and unable to reach the network.
- These types of firewalls are secure until a user accesses an unsafe site or file. Then the network is easily compromised.

Stateful Inspection Firewalls

Stateful inspection types of firewalls, also known as dynamic pack filtering, are like packet filtering firewalls, but stronger.

Scan much more than just the packet header. They are equipped to analyze a packet's content all the way through the application layer.

Look at previous communication patterns and compare incoming packets to those that have been approved in the past.

Close off any unused ports as well.

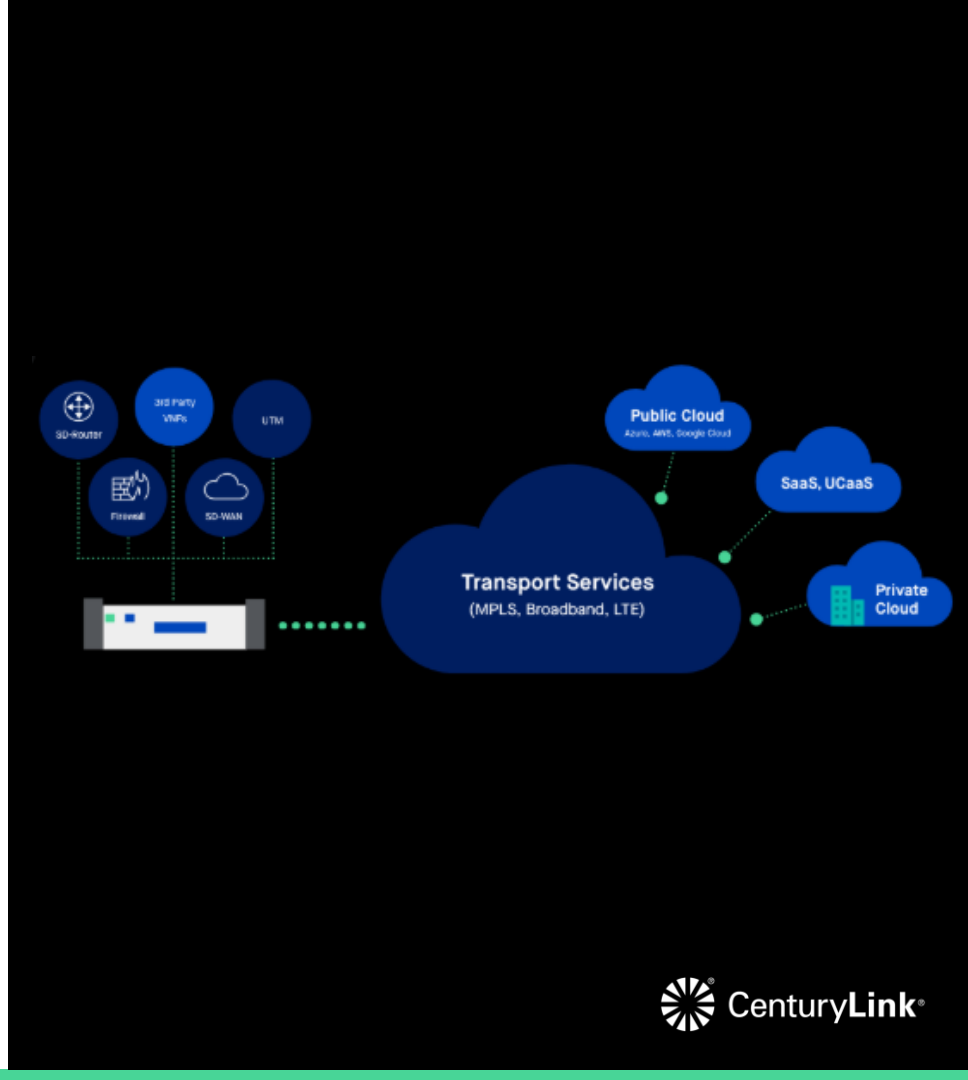
This adds another layer of protection by preventing hackers from accessing your network by spoofing port addresses that are always open.

Typically require more memory to run and can be harder to install. New connections can take much longer to load as a result.

CenturyLink

UTM Firewalls

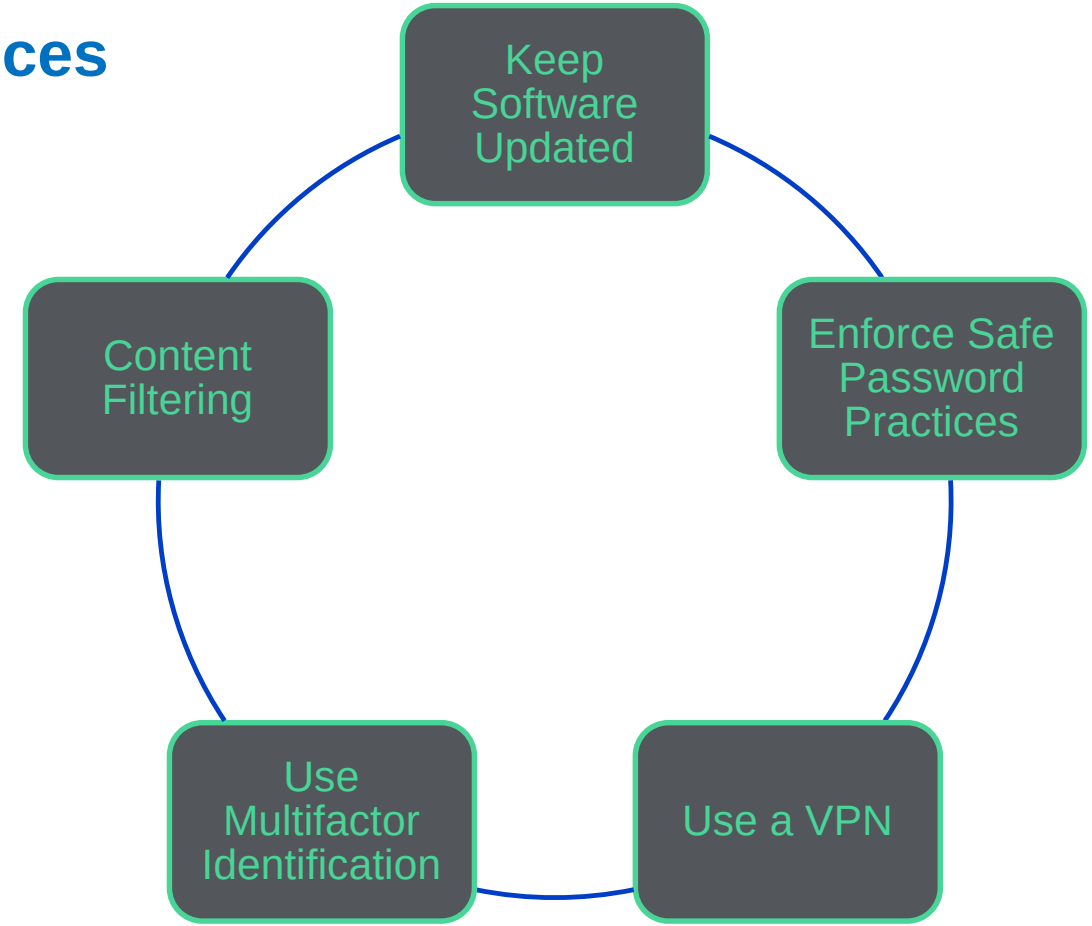
- Unified Threat Management firewalls go one step further than average firewall types because they incorporate more security programs in their design.
- Some extra features that are often available with UTM types of firewalls include anti-malware software, anti-spyware, anti-virus, VPN, and DOS/DDOS protection.



CenturyLink

Best Practices

Best Practices



CenturyLink

Questions?

www.pikespeaksbdc.org

Funded in part through a cooperative agreement with the U.S. Small Business Administration