Agenda

- VPN

VPN is short for?

VPN is short for?

Virtual Private Network

Private Network and Private IPv4 address

IP addresses reserved for organizations to use, not routable on the Internet.

- class A: 10.0.0.0 - 10.255.255.255; number of addresses: 256x256x256=16777216
- class B: 172.16.0.0 - 172.31.255.255; number of addresses: 256x256x16=1048576
- class C: 192.168.0.0 - 192.168.255.255; number of addresses: 256x256=65536

Why VPN?

- Connect two or more private networks in a secure way.
- Unblock geo-blocking, e.g., people in certain countries can't access www.youtube.com.
- Hide your identity and IP address.

VPN is said to be “virtual" because?

VPN is said to be “virtual" because?

VPN does not use a dedicated line, rather, it uses the same public Internet connections that millions of people use.

Terminology

- `VPN server`: a VPN server is configured to accept connections from clients. The VPN server is exposed to the outside network.
- `VPN client`: a VPN client can be a router that serves as the endpoint of a site-to-site VPN connections, which uses hardware to connect two networks. It can also be an operating system (OS) configured to function as an endpoint in a VPN - client-to-site VPN connection.
- `IP Tunneling`: The technology to implement VPN is called IP Tunneling, i.e., Data is sent through the VPN connection (IP Tunnel).

Site-to-site VPN

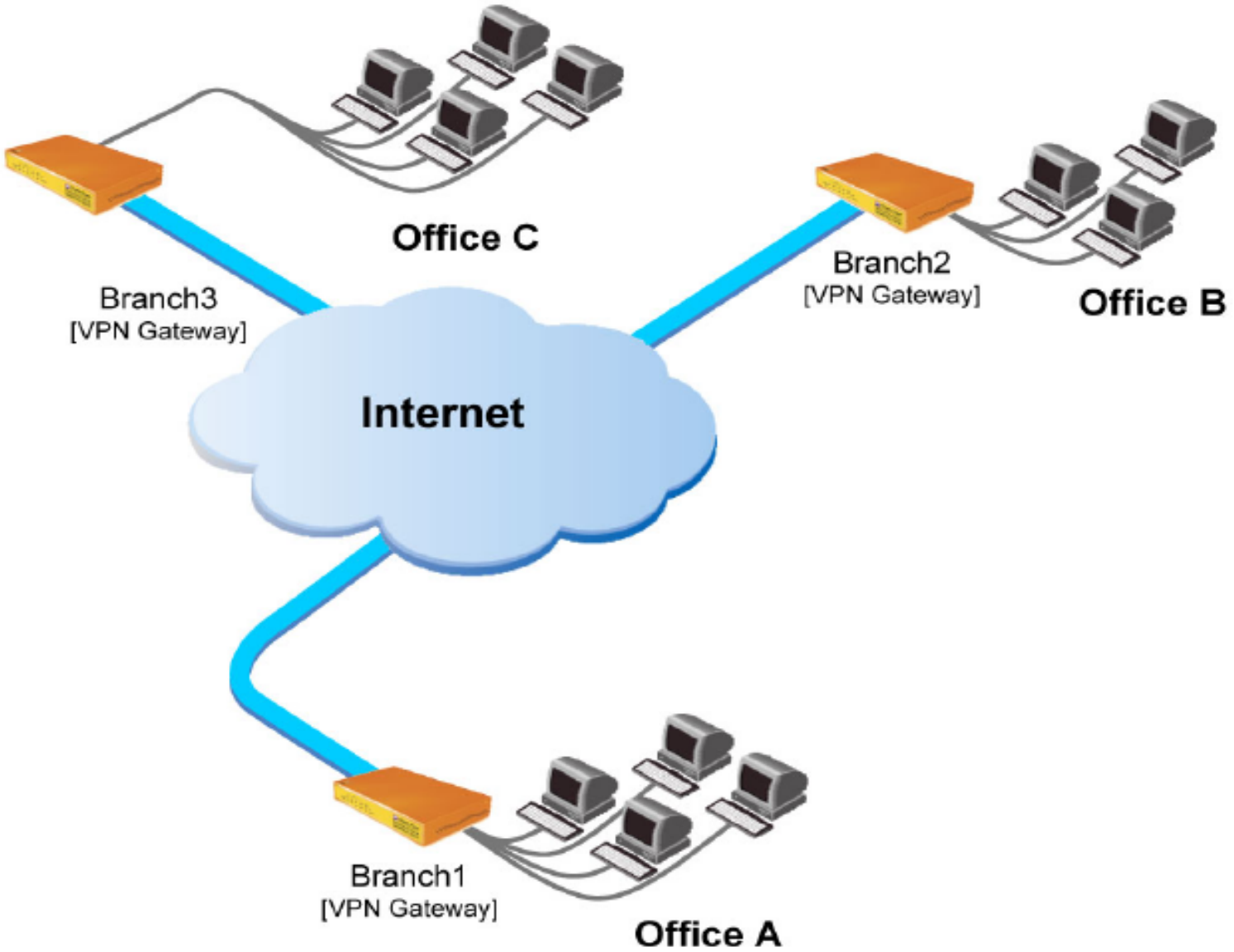
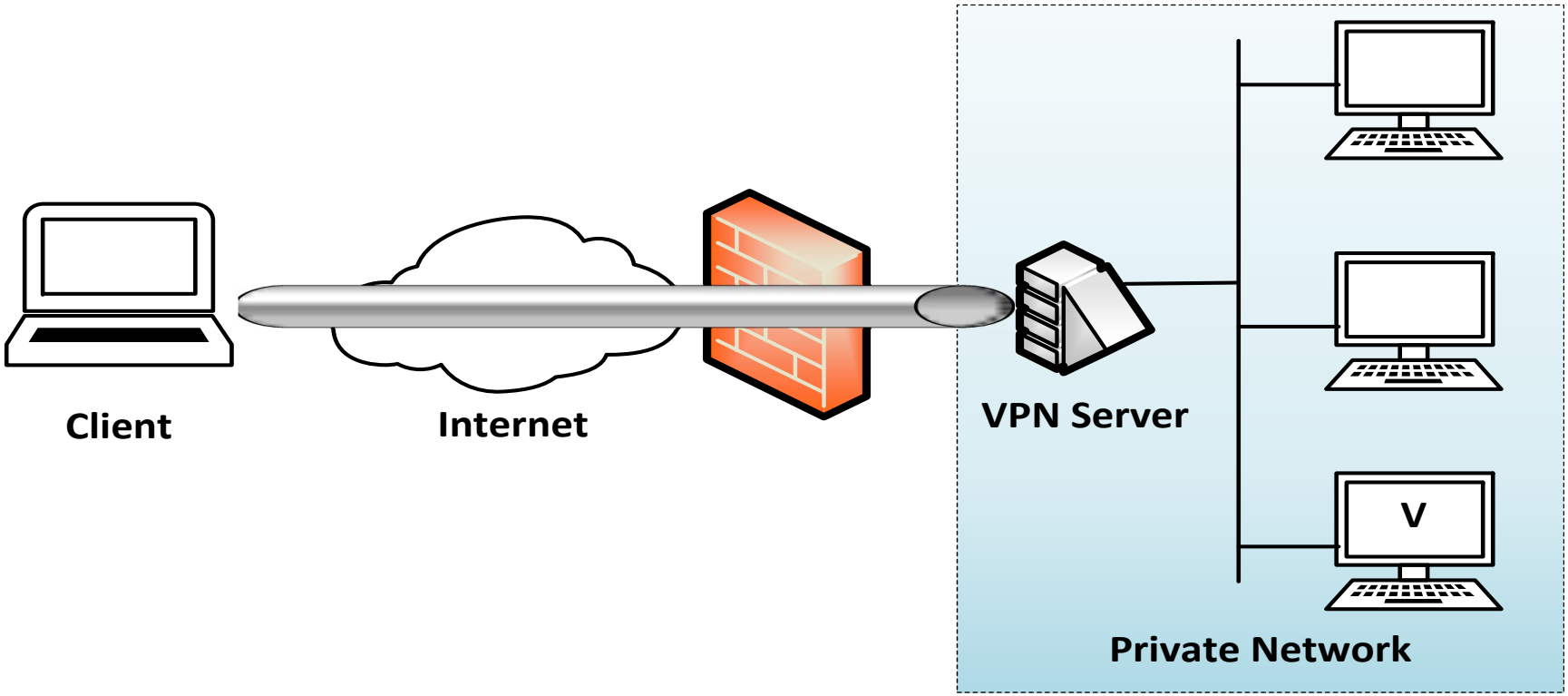


image source: checkpoint.com

Client-to-site VPN

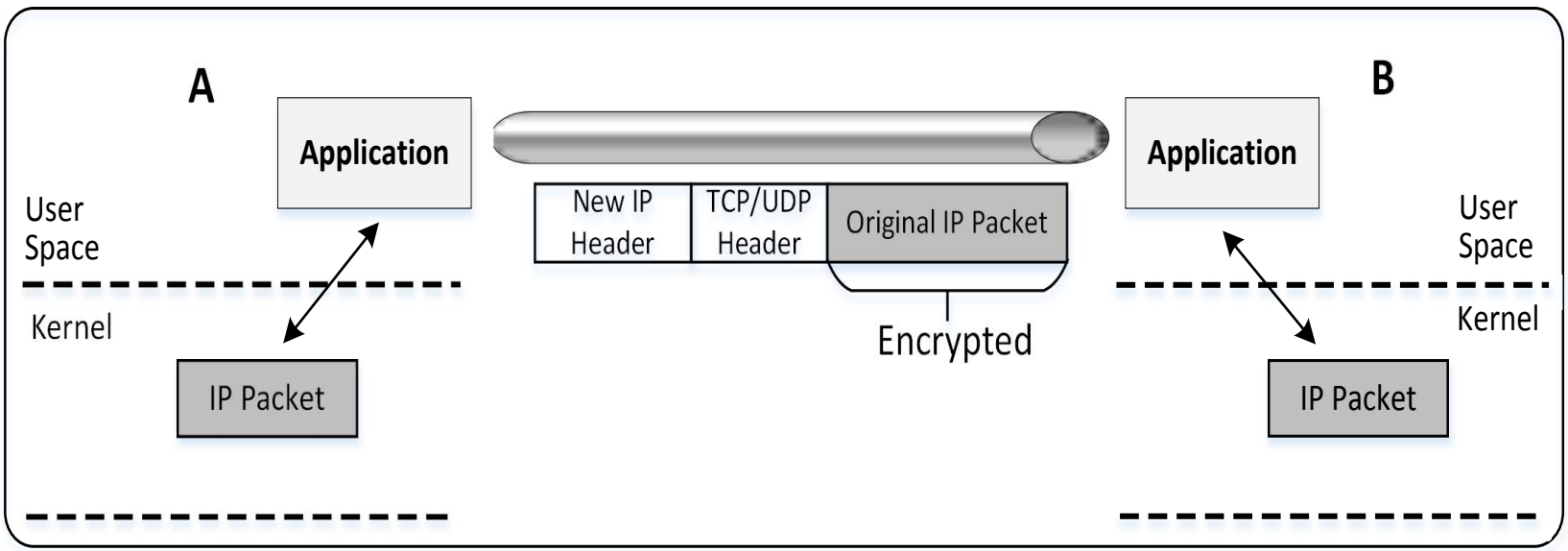


Boise State VPN Service and Policy

- Service: https://www.boisestate.edu/oit-network/vpn-services/
- Policy: https://policy.boisestate.edu/information-technology/policy-title-remote-access/

The Three VPN Core Activities

- Encapsulation: Private IP address not routable on the Internet. enclose a packet within another packet that has a different IP source and destination information.
- Encryption
- Authentication



Case Study: Use VPN Hide Identity

- Guccifer 2.0, who hacked into the Democratic National Committee (DNC) email server and then leaked to WikiLeaks in June, 2016.
- Also claimed to have hacked Democratic Congressional Campaign Committee (DCCC) (August, 2016) and Clinton Foundation (October, 2016).
- Many security experts have speculated Guccifer 2.0 is from Russia: They found that he is using the Russia-based Elite VPN service to communicate and leak documents directly with the media; Forensic examination of metadata in copies of documents distributed by Guccifer 2.0 suggest they were edited on a machine set up for a Russian language user. Also, While Guccifer 2.0 claimed that he is Romanian, but when pressed to use the Romanian language in an interview with Motherboard via online chat, "he used such clunky grammar and terminology that experts believed he was using an online translator."

References

A large portion of the material is adapted from:

- Guide to Network Defense and Countermeasures - Randy Weaver, Dawn Weaver, Dean Farwood
- Computer Security - A Hands-on Approach by Wenliang Du
- Explainer: What is a virtual private network (VPN) - theconversation.com http://theconversation.com/explainer-what-is-a-virtual-private-network-vpn-12741
- Guccifer 2.0: All Roads Lead to Russia -threatconnect.com https://www.threatconnect.com/blog/guccifer-2-all-roads-lead-russia/
- Guccifer 2.0 wikipedia page: https://en.wikipedia.org/wiki/Guccifer_2.0

Backup Slides

Who is Guccifer?

- Guccifer was the alias adopted by Marcel Lehel Lazar who, from 2013 onwards, targeted high-profile Americans, many of them politicians, and sought to hack into their personal email and social media accounts.
- In January 2014, Lazar was arrested in Romania on hacking offences and was given a four-year jail term. In March 2016, he was extradited to the US to face trial on a variety of hacking and fraud charges.
- In May 2016, while in jail, he told Fox News that he had repeatedly broken into a private email server set up by Hillary Clinton that handled her electronic correspondence.
- Clinton has denied the server was hacked and the US State Department said it could find no evidence supporting Lazar's claim.
- Lazar said the Guccifer name comes from simply combining the Italian fashion brand Gucci with the name the Bible gives to the devil, Lucifer, before he was cast out.