Network Layer Security

Applied Network security (comp420 –001)

Department of Computer science

Fall 2020

IP Security Protocol (IPsec)

- The IP security protocol, more commonly known as IPsec, provides security at the network layer.
- IPsec secures IP datagrams between any two network-layer entities, including hosts and routers.
- As we will see in the next slides, many institutions (corporations, government branches, non-profit organizations, and so on) use IPsec to create virtual private networks (VPNs) that run over the public Internet.
- Let's see what it means to provide **confidentiality** at the network layer?
  - With network-layer confidentiality between a pair of network entities (for example, between two routers, between two hosts, or between a router and a host), the sending entity encrypts the payloads of all the datagrams it sends to the receiving entity.
  - The encrypted payload could be a TCP segment, a UDP segment, an ICMP message, and so on.
  - If such a network-layer service were in place, all data sent from one entity to the other—including e-mail, Web pages, TCP handshake messages, and management messages (such as ICMP and SNMP)—would be hidden from any third party that might be sniffing the network. For this reason, network-layer security is said to provide "**blanket coverage**."

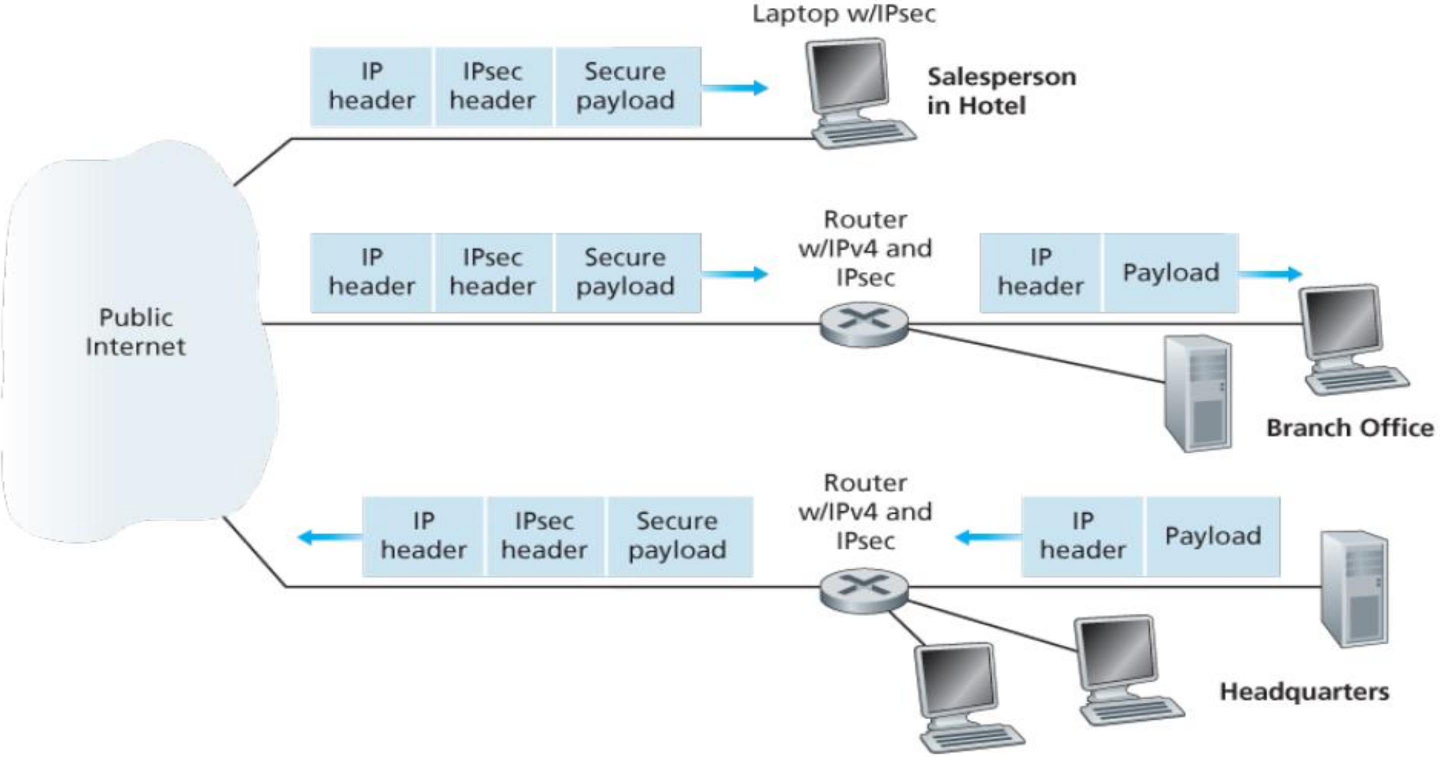
IPsec (Cont.) & Replay Attack

- What else IPsec can provide in terms of our security goals?
  - It could provide **source authentication**, so that the receiving entity can verify the source of the secured datagram.
  - A network-layer security protocol could provide data **integrity**, so that the receiving entity can check for any tampering of the datagram that may have occurred while the datagram was in transit.
  - A network-layer security service could also provide **replay-attack prevention**, meaning that Bob could detect any duplicate datagrams that an attacker might insert.
- Kaspersky says: A replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. The added danger of replay attacks is that a hacker doesn't even need advanced skills to decrypt a message after capturing it from the network. The attack could be successful simply by resending the whole thing.
- How a replay attack Works
- Consider this real-world example of an attack. A staff member at a company asks for a financial transfer by sending an encrypted message to the company's financial administrator. An attacker eavesdrops on this message, captures it, and is now in a position to resend it. Because it's an authentic message that has simply been resent, the message is already correctly encrypted and looks legitimate to the financial administrator.
- In this scenario, the financial administrator is likely to respond to this new request unless he or she has a good reason to be suspicious. That response could include sending a large sum of money to the attacker's bank account.

IPsec & Virtual Private Network (VPN)

- An institution that extends over multiple geographical regions often desires its own IP network:
- To achieve this goal, the institution could deploy a stand-alone physical network.
- Such a disjoint network, dedicated to a particular institution, is called a **private network**.
- Not surprisingly, a private network can be very costly.

- Instead of deploying and maintaining a private network, many institutions today create VPNs over the existing public Internet.
- The inter-office traffic is encrypted before it enters the public Internet.



AH and ESP Protocols

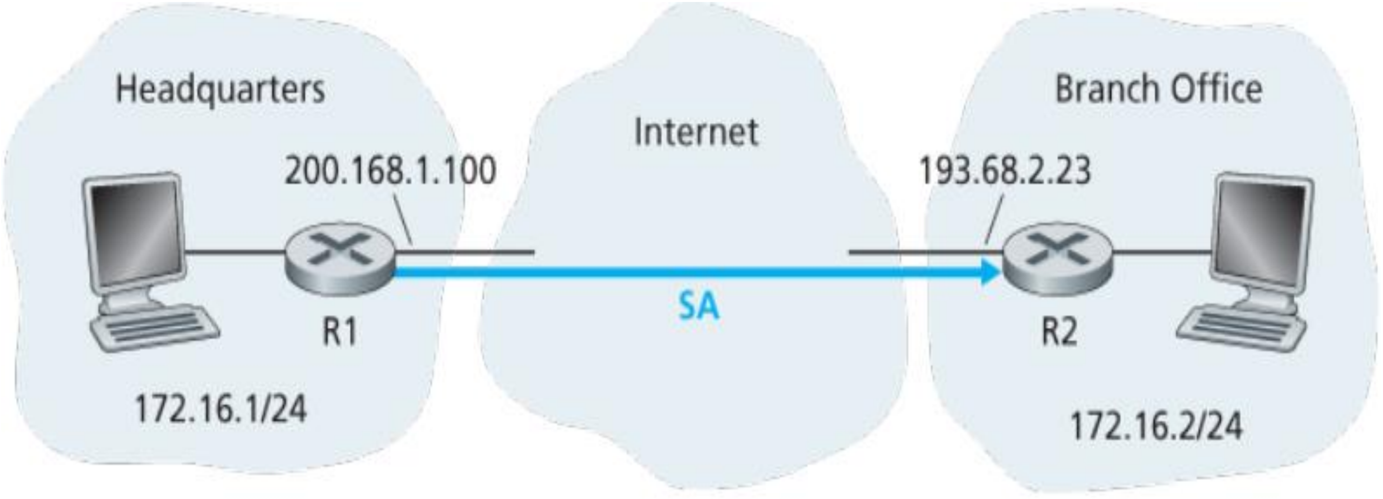
- In the IPsec protocol suite, there are two principal protocols:
  - The **Authentication Header (AH)** protocol
  - The **Encapsulation Security Payload (ESP)** protocol.
- The AH protocol provides **source authentication** and **data integrity** but does not provide confidentiality.
- The ESP protocol provides **source authentication, data integrity**, and **confidentiality**. Because confidentiality is often critical for VPNs and other IPsec applications, the ESP protocol is much more widely used than the AH protocol.

Security Association

- IPsec datagrams are sent between pairs of network entities, such as between two hosts, between two routers, or between a host and router.
- Before sending IPsec datagrams from the source entity to the destination entity, the source and destination entities create a network-layer logical connection.
- This logical connection is called a **security association (SA)**.
- A SA is a simple logical connection; that is, it is unidirectional from source to destination. If both entities want to send secure datagrams to each other, then two SAs (that is, two logical connections) need to be established, one in each direction.

Security Association (Cont.)

- Let’s see what is going on insides a SA (from router R1 to router R2):
- Router R1 will maintain the state information about this SA, which will include:
  - A 32-bit identifier for the SA, called the **Security Parameter Index (SPI)**
  - The origin interface of the SA (in this case 200.168.1.100) and the destination interface of the SA (in this case 193.68.2.23)
  - The type of encryption to be used (for example, 3DES)
  - The encryption key
  - The type of integrity check (for example, HMAC with MD5)
  - The authentication key

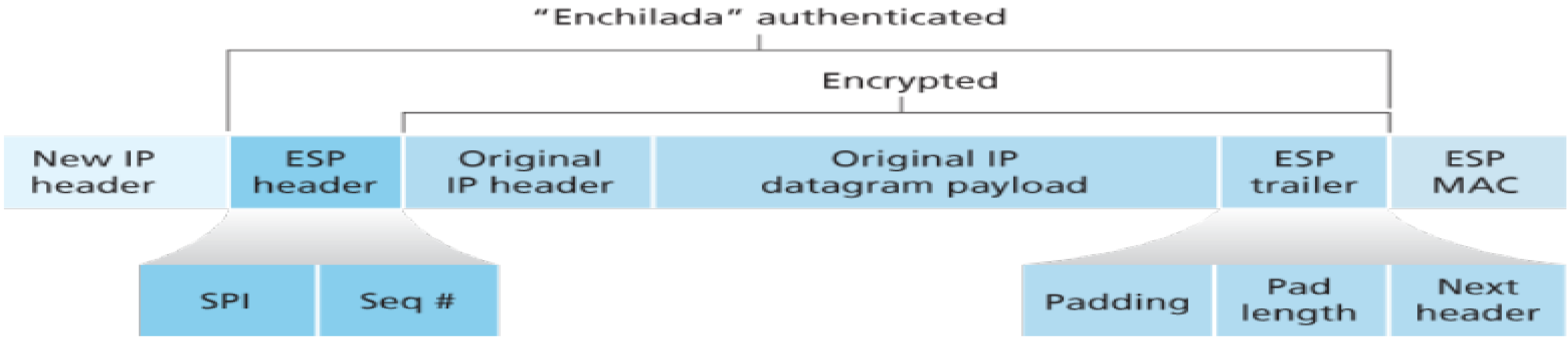


- An IPsec entity stores the state information for all of its SAs in its **Security Association Database (SAD)**, which is a data structure in the entity’s OS kernel.

The IPsec Datagram

- IPsec has two different packet forms:
  - One for the so-called **tunnel mode** (more appropriate for VPNs)
  - The other for the so-called **transport mode**
- Suppose router R1 receives an ordinary IPv4 datagram from host 172.16.1.17 (in the headquarters network) which is destined to host 172.16.2.48 (in the branch-office network).
- Router R1 uses the following recipe to convert this “original IPv4 datagram” into an IPsec datagram:

The IPsec Datagram (Cont.)



- Appends to the back of the original IPv4 datagram (which includes the original header fields!) an
- "ESP trailer" field
- Encrypts the result using the algorithm and key specified by the SA
- Appends to the front of this encrypted quantity a field called "ESP header"; the resulting package iscalled the "**Enchilada**"
- Creates an authentication MAC over the whole enchilada using the algorithm and key specified in the SA
- Appends the MAC to the back of the enchilada forming the payload
- Finally, creates a brand new IP header with all the classic IPv4 header fields (together normally 20 bytes long), which it appends before the payload

The IPsec Datagram (Cont.)

- Note that the resulting IPsec datagram is an IPv4 datagram, with the traditional IPv4 header fields followed by a payload.
- But in this case, the payload contains an ESP header, the original IP datagram, an ESP trailer, and an ESP authentication field (with the original datagram and ESP trailer encrypted).
- The original IP datagram has 172.16.1.17 for the source IP address and 172.16.2.48 for the destination IP address. Because the IPsec datagram includes the original IP datagram, these addresses are included (and encrypted) as part of the payload of the IPsec packet.

Your Turn 1

What about the source and destination IP addresses that are in the new IP header, that is, in the left-most header of the IPsec datagram?

The IPsec Datagram (Cont.)

- As you might expect, they are set to the source and destination router interfaces at the two ends of the tunnels.
- Also, the protocol number in this new IPv4 header field is not set to that of TCP, UDP, or SMTP, but instead to 50, designating that this is an IPsec datagram using the ESP protocol.
- After R1 sends the IPsec datagram into the public Internet, it will pass through many routers before reaching R2. Each of these routers will process the datagram as if it were an ordinary datagram—they are completely oblivious to the fact that the datagram is carrying IPsec-encrypted data.
- For these public Internet routers, because the destination IP address in the outer header is R2, the ultimate destination of the datagram is R2.

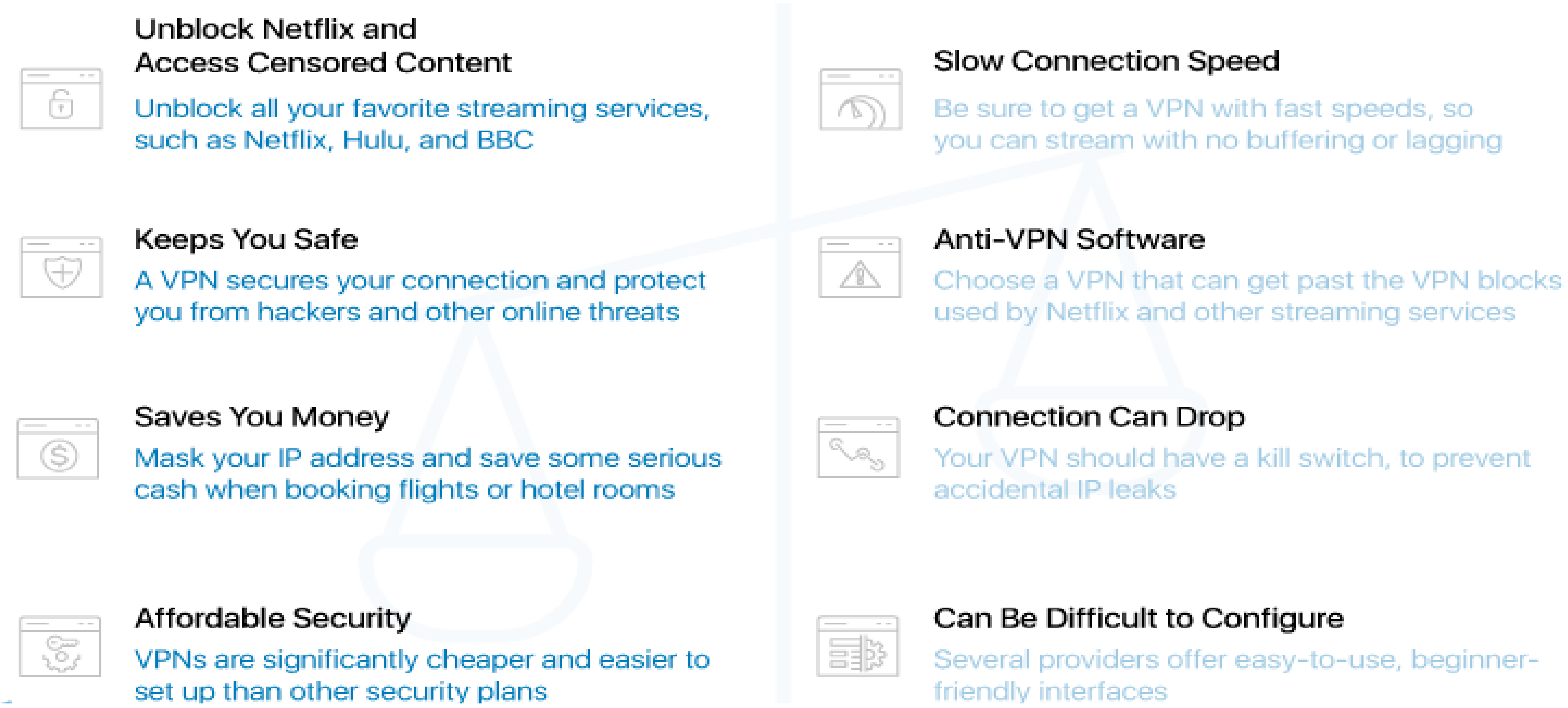
Virtual Private Network (VPN) - Introduction

- A Virtual Private Network (VPN) is a tunnel connecting two different networks.

- VPN extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

- There are two types of VPN
  - Remote-access VPN
  - Site-to-site VPN

VPN Pros vs. Cons



Pros

Unblock Netflix and Access Censored Content

Unblock all your favorite streaming services, such as Netflix, Hulu, and BBC

Keeps You Safe

A VPN secures your connection and protect you from hackers and other online threats

Saves You Money

Mask your IP address and save some serious cash when booking flights or hotel rooms

Affordable Security

VPNs are significantly cheaper and easier to set up than other security plans

Cons

Slow Connection Speed

Be sure to get a VPN with fast speeds, so you can stream with no buffering or lagging

Anti-VPN Software

Choose a VPN that can get past the VPN blocks used by Netflix and other streaming services

Connection Can Drop

Your VPN should have a kill switch, to prevent accidental IP leaks

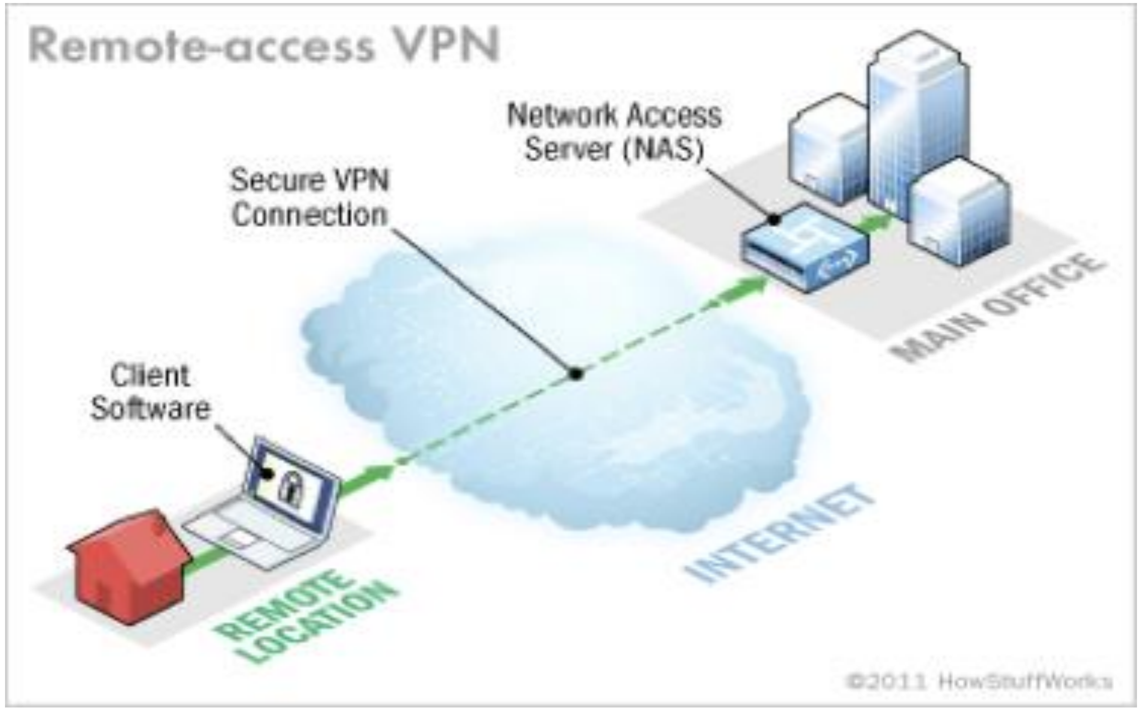
Can Be Difficult to Configure

Several providers offer easy-to-use, beginner-friendly interfaces

Remote-access VPN

- A remote-access VPN allows individual users to establish secure connections with a remote computer network.

- Those users can access the secure resources on that network as if they were directly plugged in to the network's servers.

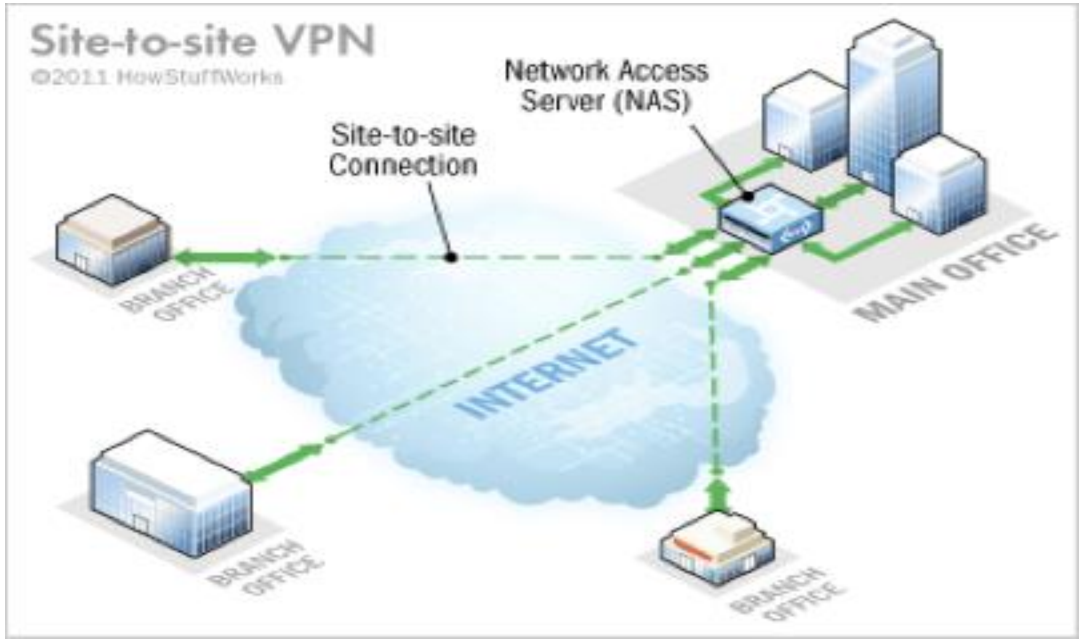


- Another name for this type of VPN is virtual private dial-up network (VPDN), acknowledging that in its earliest form, a remote-access VPN required dialing in to a server using an analog telephone system.

- Example: NCAT VPN allows us to access library resources as if we are on campus.

Site-to-site VPN

- A site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the internet.



- Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations.

- An example of a company that needs a site-to-site VPN is a growing corporation with dozens of branch offices around the world.

VPN Tunneling

- Most VPNs rely on tunneling to create a private network that reaches across the Internet
- **Tunneling** is the process of placing an entire packet within another packet before it's transported over the Internet
  - That outer packet protects the contents from public view and ensures that the packet moves within a virtual tunnel. This layering of packets is called **encapsulation**.
  - Computers or other network devices at both ends of the tunnel, called **tunnel interfaces**, can encapsulate outgoing packets and reopen incoming packets.
  - Users (at one end of the tunnel) and IT personnel (at one or both ends of the tunnel) configure the tunnel interfaces they're responsible for to use a **tunneling protocol**.
  - Also called an **encapsulation protocol**, a **tunneling protocol** is a standardized way to encapsulate packets

Equipment Used in a VPN

- While a VPN can be configured on generic computer equipment such as standard servers, most businesses opt for dedicated equipment optimized for the VPN and general network security.

- There is no standard that all VPNs follow in terms of their setup. When planning or extending a VPN, though, the following equipment should be considered:
  - **Network access server**
  - **Firewall**
  - **AAA Server:** One widely used standard for AAA servers is Remote Authentication Dial-in User Service (RADIUS). When a RADIUS server is part of a VPN, it handles authentication for all connections coming through the VPN's NAS.

- In practice, a small company might have all of its VPN equipment on site or might outsource its VPN services to an enterprise service provider. A larger company with branch offices might choose to co-locate some of its VPN equipment, meaning that it will set up that equipment in a co-location facility (or colo). A colo is a large data center that rents space to businesses that need to set up servers and other network equipment on a very fast, highly reliable Internet connection.

VPN Encryption and Security Protocols

- VPN needs more than just a pair of keys to apply encryption. That's where protocols come in. A site-to-site VPN could use either Internet protocol security protocol (IPSec) or generic routing encapsulation (GRE).
- **GRE** provides the framework for how to package the passenger protocol for transport over the Internet protocol (IP). This framework includes information on what type of packet you're encapsulating and the connection between sender and receiver.
- **IPSec** is a widely used protocol for securing traffic on IP networks, including the Internet. IPSec can encrypt data between various devices, including router to router, firewall to router, desktop to router, and desktop to server.

VPN Protocols

- **OpenVPN:** Open source, offers strongest encryption, suitable for all activities, a little slow at times
- **L2TP/IPSec:** Widely used protocol, good speeds, but easily blocked due to reliance on single port
- **SSTP:** Good security, essentially a Microsoft-developed proprietary protocol
- **IKEv2/IPSec:** Fast, mobile friendly, with several open source implementations
- **PPTP:** Fast, widely supported, but full of security holes, only use for streaming and basic web browsing

VPN Security Concerns

- In the real-world VPN providers are not all cut from the same cloth and can compromise user's security and privacy through the following means:

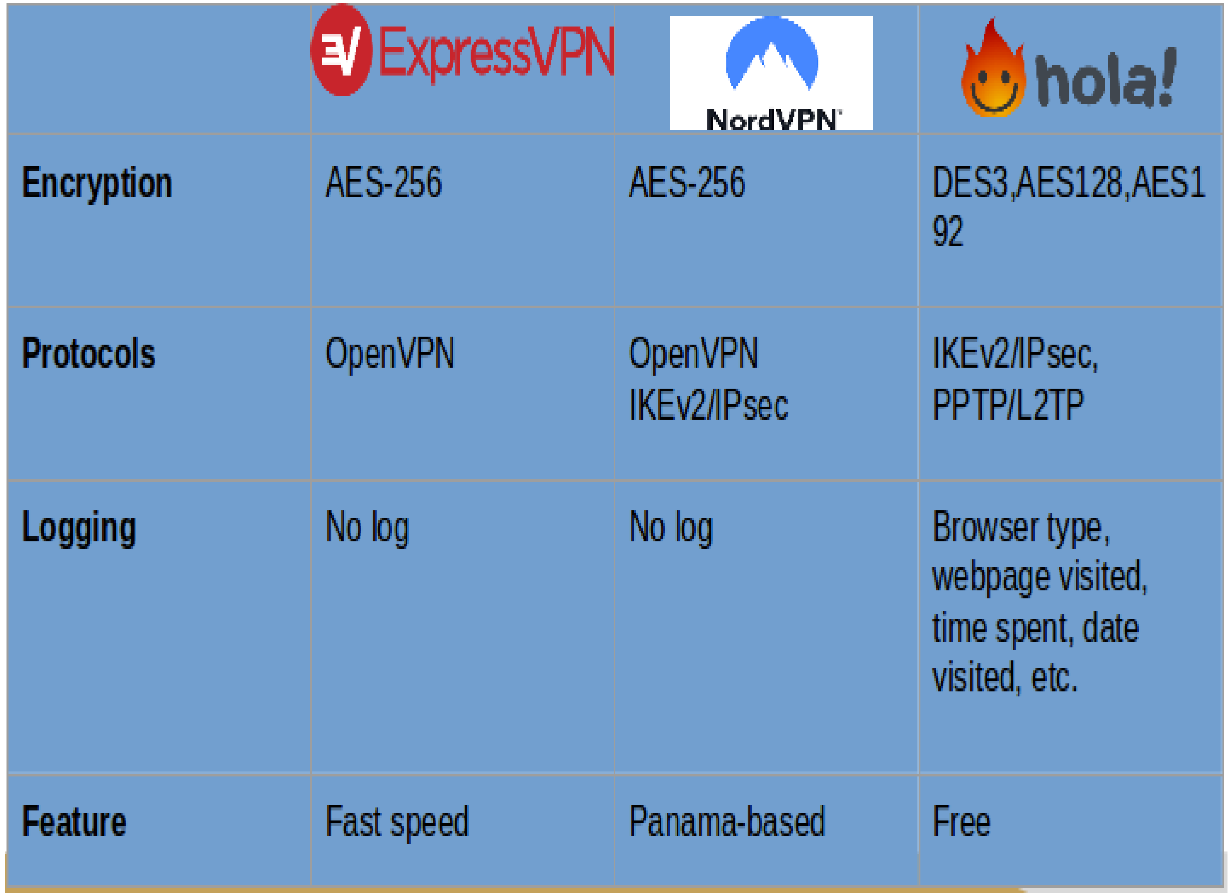
- **Logging** (ie. traffic logs, connection logs, IP addresses, metadata)
- **Tracking, ad injection, and malware** (ie. using/mining with browser cookies to insert adverts, collect browsing data, share with ad exchange, or malware payloads to infect user's to perform unintended action)
- **Insufficient security** (ie. encryption - channel encryption/authentication/key exchange, leak protection - WebRTC leak/connection disruption)

- For example, Hola VPN, offends a majority of the above

How would you know a VPN is good?

- You do have to trust that your VPN service provider has your best interests at heart, because you're relying on them to secure your connection, keep everything encrypted, and to protect your activity from prying eyes.

- Things to look out for when choosing a VPN:
  - Country of Origin
  - Activity Logging
  - Terms of Service
  - VPN protocols
  - Leak Test
  - Be aware of Free Service
  - Anonymous Payment option



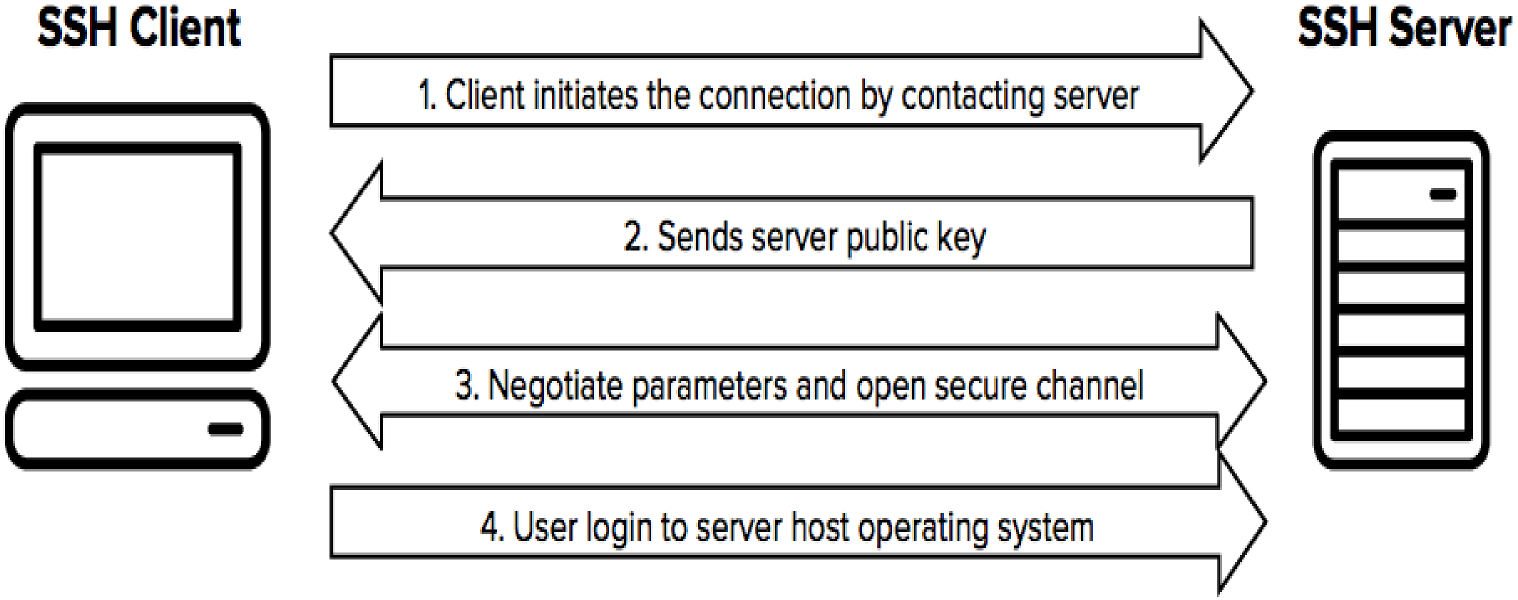
	ExpressVPN	NordVPN	hola!
Encryption	AES-256	AES-256	DES3,AES128,AES192
Protocols	OpenVPN	OpenVPN IKEv2/IPsec	IKEv2/IPsec, PPTP/L2TP
Logging	No log	No log	Browser type, webpage visited, time spent, date visited, etc.
Feature	Fast speed	Panama-based	Free

Secure Shell (SSH)

- What happens when a system administrator needs to log into a machine securely to be able to administrate it?
- In this case, the system administrators will want to have access to a shell, or a terminal program, and needs to find a way to connect to the server in order to remotely have access to a shell in order to execute commands and provide administrative functions.
- In the past, a system administrator would connect to a server with an application called Telnet. However, the traffic between the client machine and the server machine was insecure (in plain text).
- The Secure Shell, or SSH, is based on TLS and uses a shared secret between the server and the client to establish a secure connection between the two.

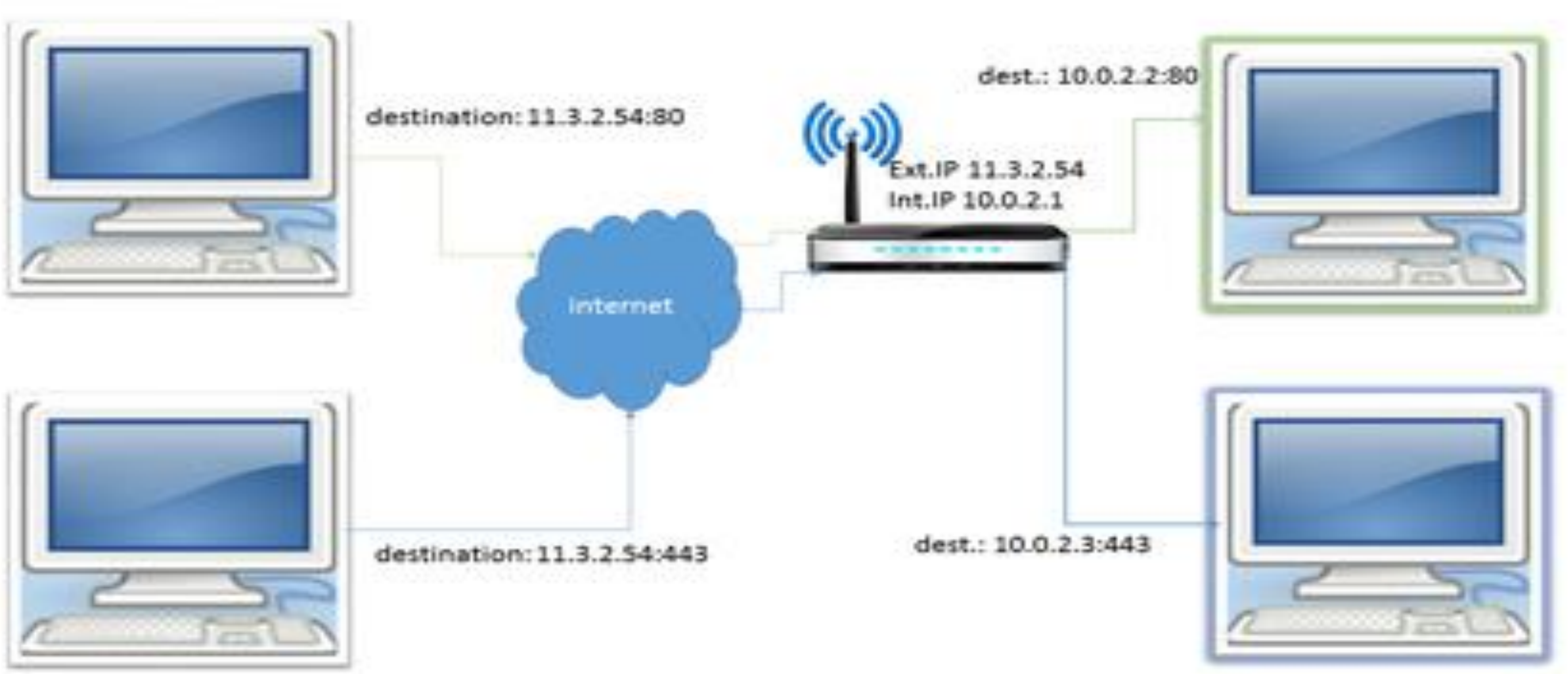
Quick Overview of how SSH works

1. Client puts their public key on the server
2. Client Connects to the server
3. Server responds with secret
4. Client responds to verify the secret
5. Secure Tunnel established.


SSH Client
SSH Server
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system

Port Forwarding

- Another aspect of SSH is **port forwarding** .
- **port forwarding,** or **port mapping** redirects a communication request from one address and port number combination (socket) to another while the packets are traversing a network gateway, such as a router or firewall.
- It is commonly used in the gaming, security camera setup, voice over ip, and downloading files.



Trust On First Use (TOFU)

- SSH relies on a trust model called TOFU.
- SSH doesn't require third party signed certificates and everything is handled entirely between the SSH client and server.
- The idea behind trust on first use is that the first connection between the client and the server is trusted. In fact, SSH client blindly trusts first connection to the SSH server and this is why it's called trust on first use.
- Then it is assumed that the subsequent communications can be also trusted. So if that first connection isn't trusted, then all the subsequent interactions are not going to be trusted.
- TOFU (Trust on First Use)
  - Alternative to TLS trust model
  - Blindly trusts server on the first connection
  - Security as good as the first connection