Connecting Remote Sites Securely using an Router Based IPsec Virtual Private Network

Ryan Tallent

Department of Integrated Information Technology
University of South Carolina

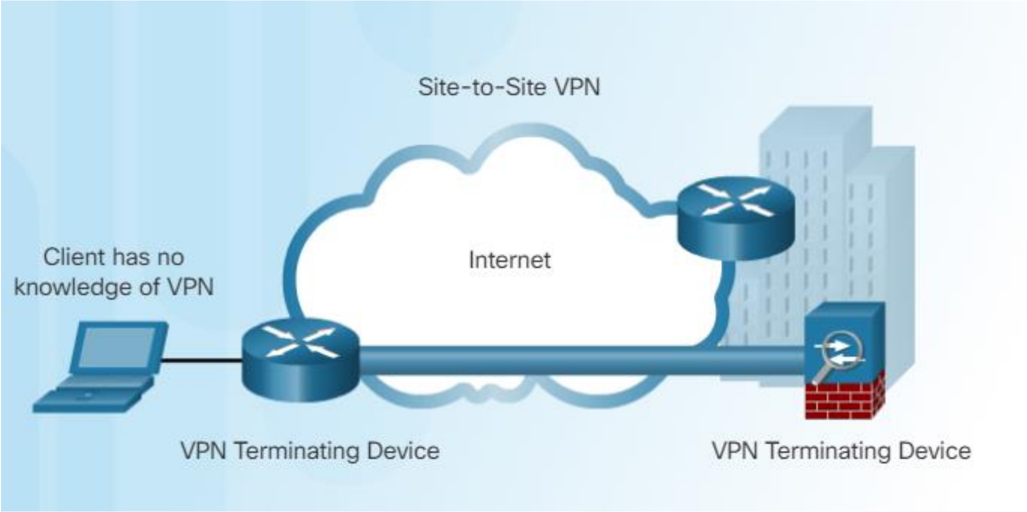
December 2020

Agenda

- Introduction to network security and confidentiality
- Background information
  - Generic Routing Encapsulation (GRE)
  - IPsec Virtual Private Networks (VPN)
- Implementation of hybrid system using GRE and IPsec
- Conclusion

Introduction

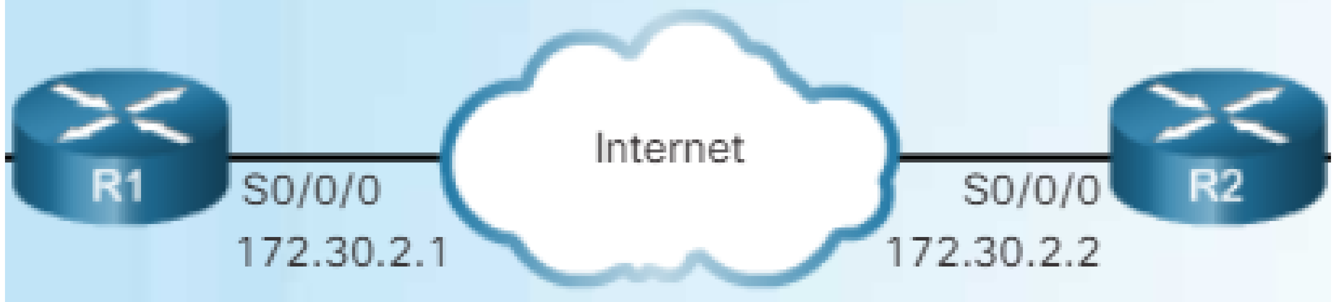
- Network communication frequently relies on Internet Service Provider (ISP) networks or other untrusted network connections to carry the information to its destination.
- In order to enable secure communication between two networks, which are separated by a public network (e.g., the Internet), encryption is required.
- Site-to-site virtual private networks (VPN) enable remote sites to communicate confidentially, using cryptographic techniques (encryption, hash functions).



Cisco CCNA Security Chapter 8.1.2.3

Problem Description

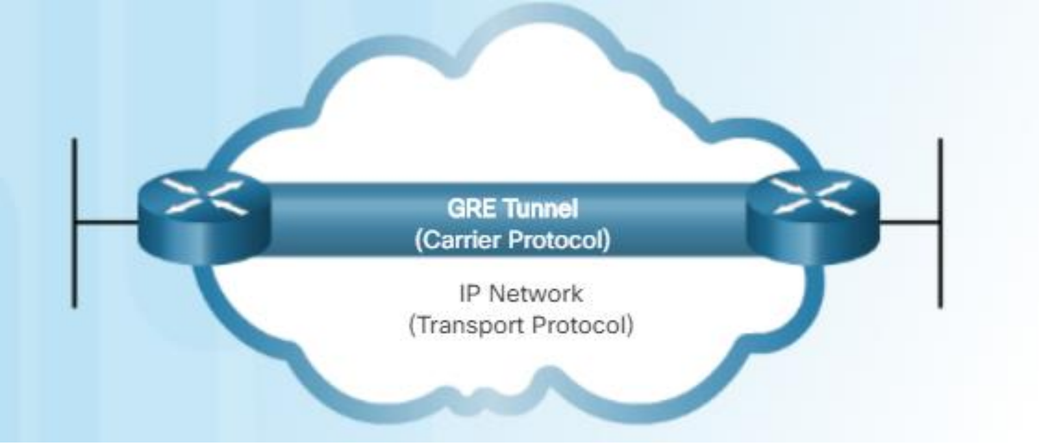
- When communications travel past the local router and onto untrusted networks, they become much more vulnerable to falling into the wrong hands.



Cisco Routing and Switching Essentials Page 8.3.1.3

Background Information

- Generic Routing Encapsulation (GRE) allows remote networks to be discovered through dynamic routing advertisements.

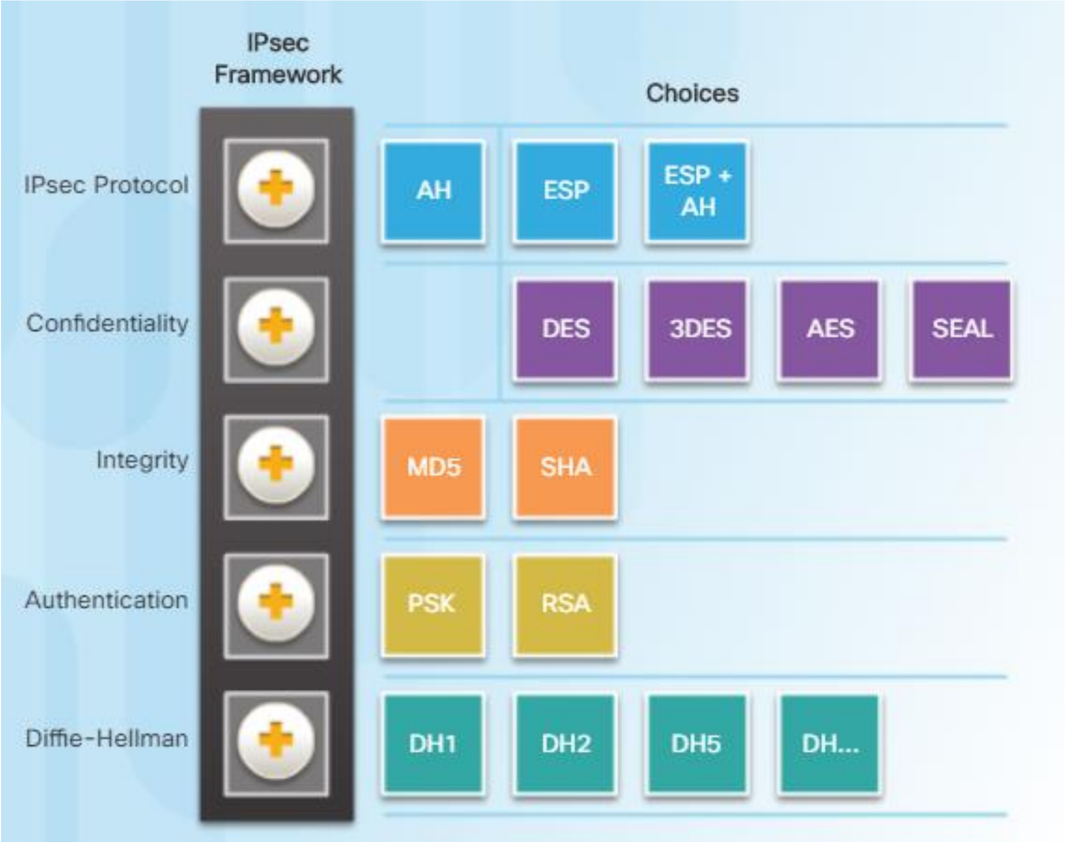


Cisco CCNA Security Chapter 8.3.1.5

- GRE enables broadcast and multicast traffic to be transmitted to the remote end point via the GRE tunnel

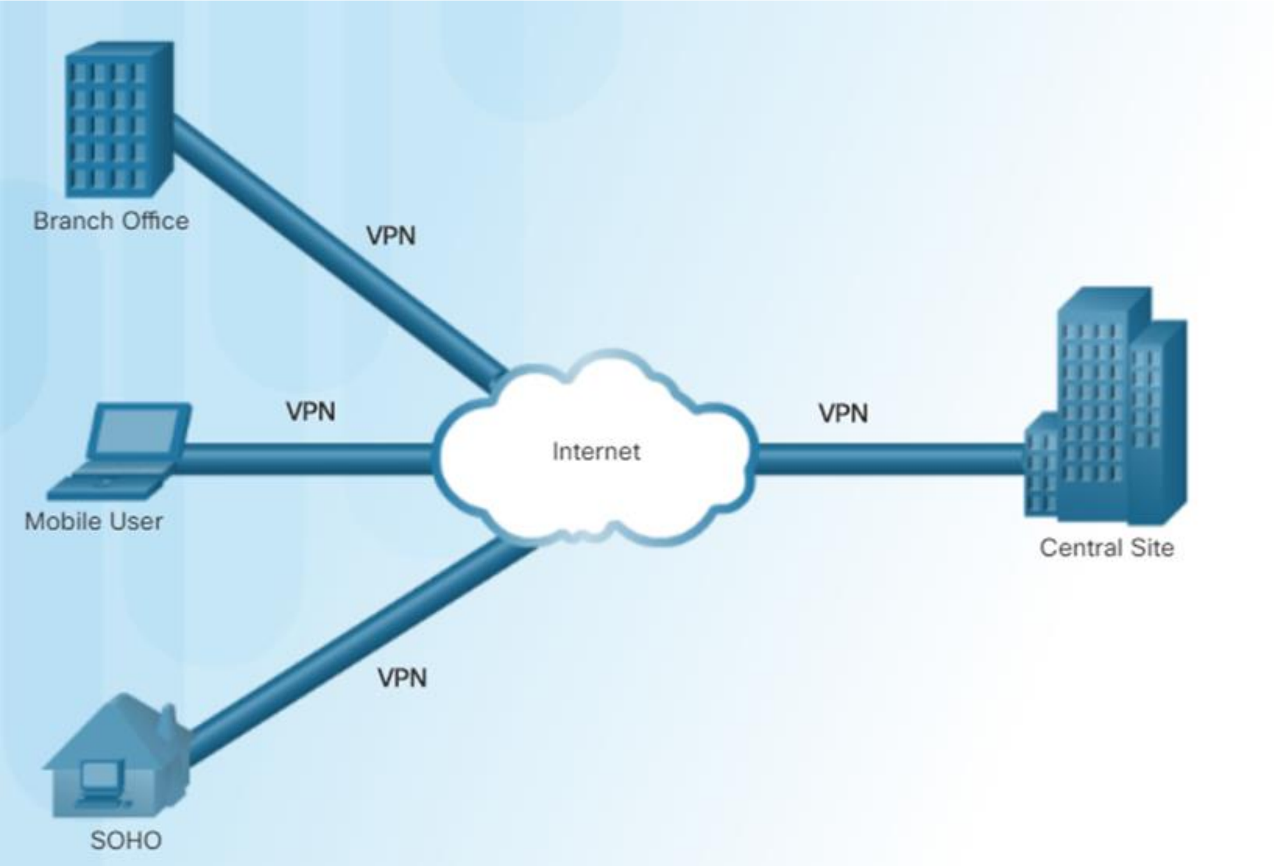
Background Information

- IP security (IPsec) is a standard framework composed of five building blocks
  - Protocol: encapsulation protocol carrying the data
  - Confidentiality: encryption algorithm used for privacy
  - Integrity: hash function used for integrity control
  - Authentication: mechanism used to ensure the identity of the two end points of the VPN
  - Diffie-Hellman: algorithm used to create the keys used to encrypt the data
- IPsec only works with unicast transmissions



Cisco CCNA Security Chapter 8.2.1.1

Proposed Solution and Implementation

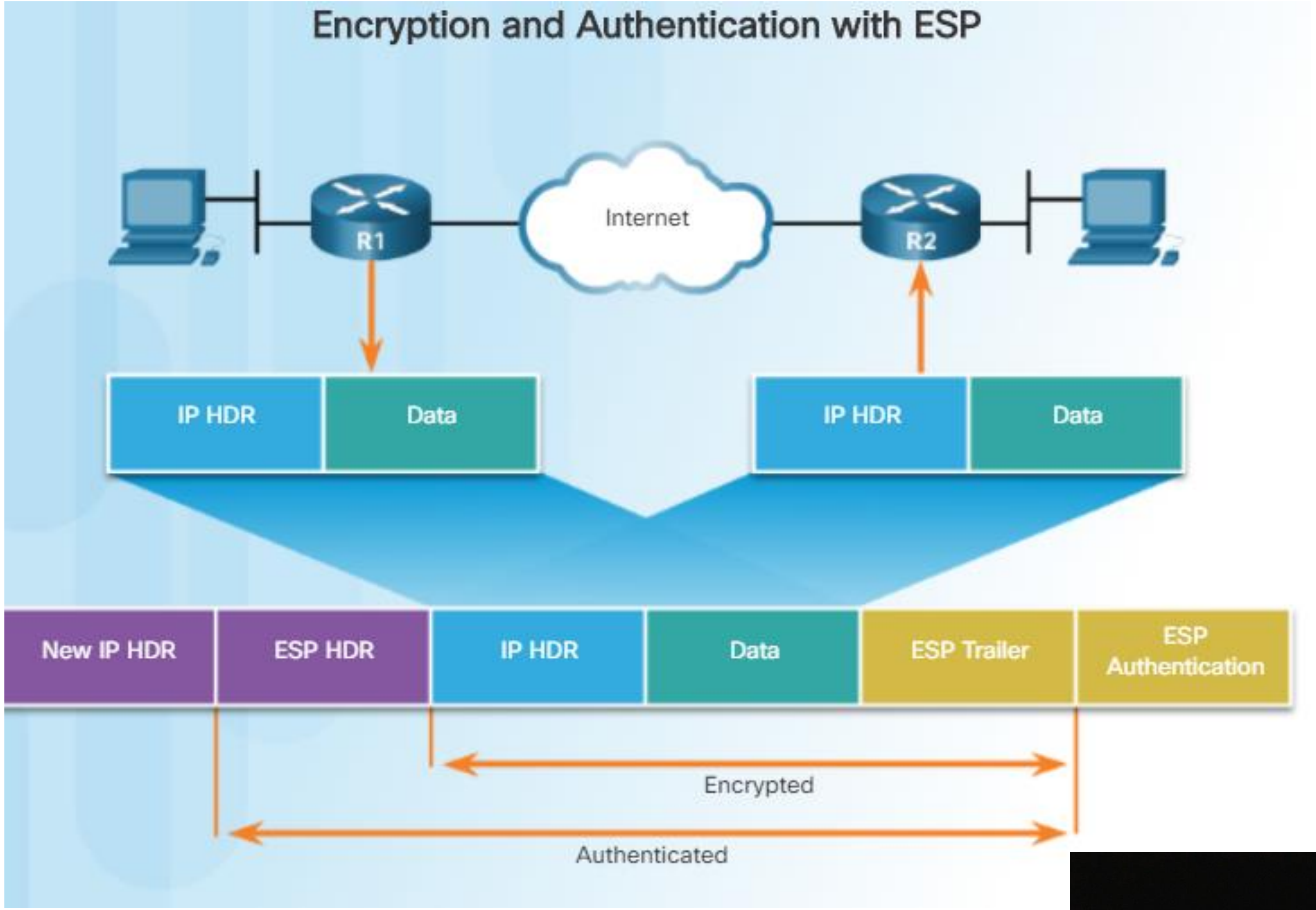


Cisco CCNA Security Chapter 8.1.1.2

- The combination of the GRE and VPN is necessary to accomplish the task of transmitting data securely. GRE will create an envelop for the data to be transmitted through untrusted networks. The IPsec protocol, encapsulation security payload (ESP), is the means of sealing that envelop and protecting its contents from being changed or compromised

Establish VPN

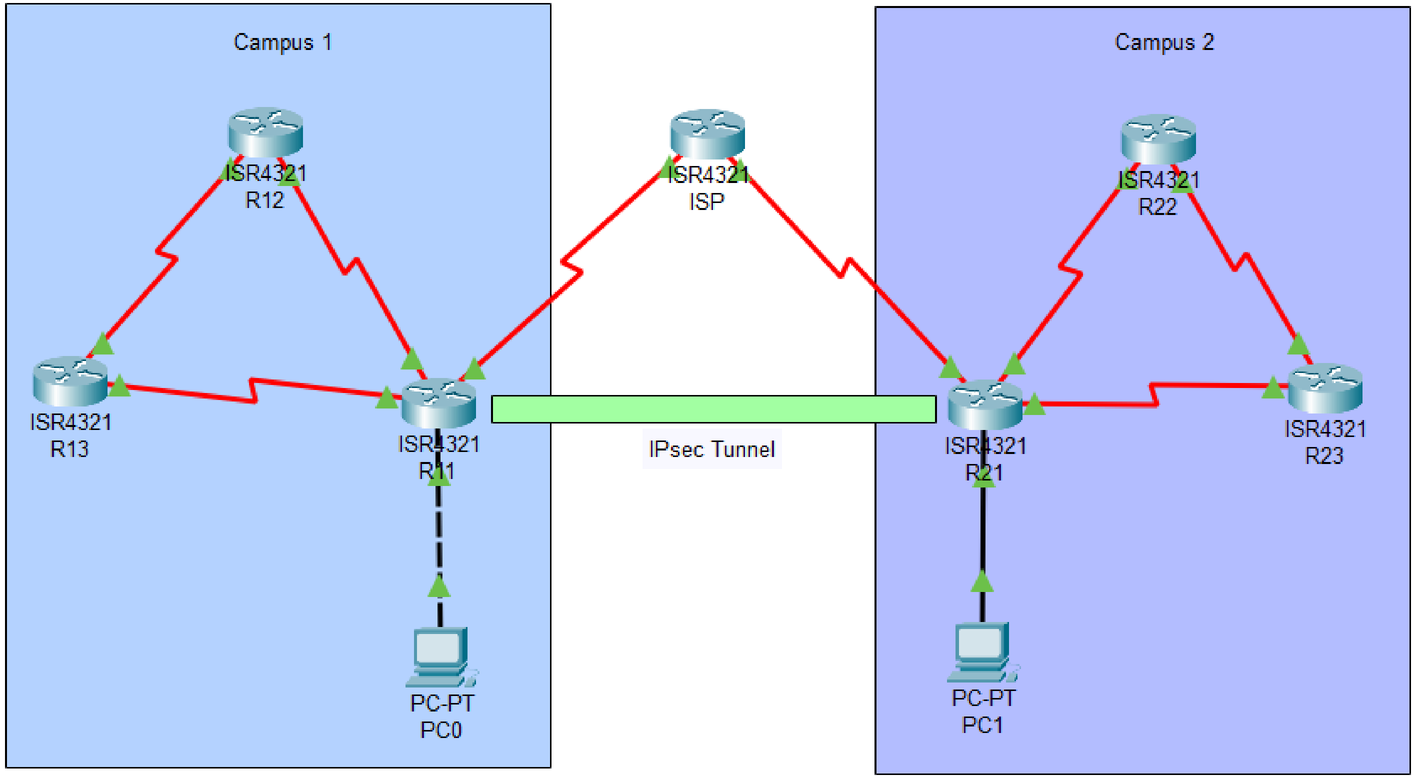
- The VPN enables information to be securely transmitted across the Internet. The communicating hosts can be assured their data is private, intact, and sent from a verified and trustworthy source.



Cisco CCNA Security Chapter 8.2.2.4

Conclusion

- Through the implementation of a VPN, a high level of security and privacy can be achieved. The likelihood of information being intercepted, tampered with, or compromised by malicious outside actors is greatly reduced.


Campus 1
ISR4321
R12
ISR4321
R13
ISR4321
R11
PC-PT
PC0
ISR4321
ISP
IPsec Tunnel
Campus 2
ISR4321
R22
ISR4321
R21
ISR4321
R23
PC-PT
PC1