Connecting Remote Sites Securely using IPSec Virtual Private Network and Next-generation Firewalls

Nathan Bohmer, Josue Hernandez
Advisor: Jorge Crichigno

Department of Integrated Information Technology
University of South Carolina

December 2020

Agenda

- Introduction
- Problem description
- Background information
  - Next-generation Firewalls (NGFWs)
  - IPSec Virtual Private Networks (VPNs)
- Proposed solution and implementation
- Conclusion

Introduction

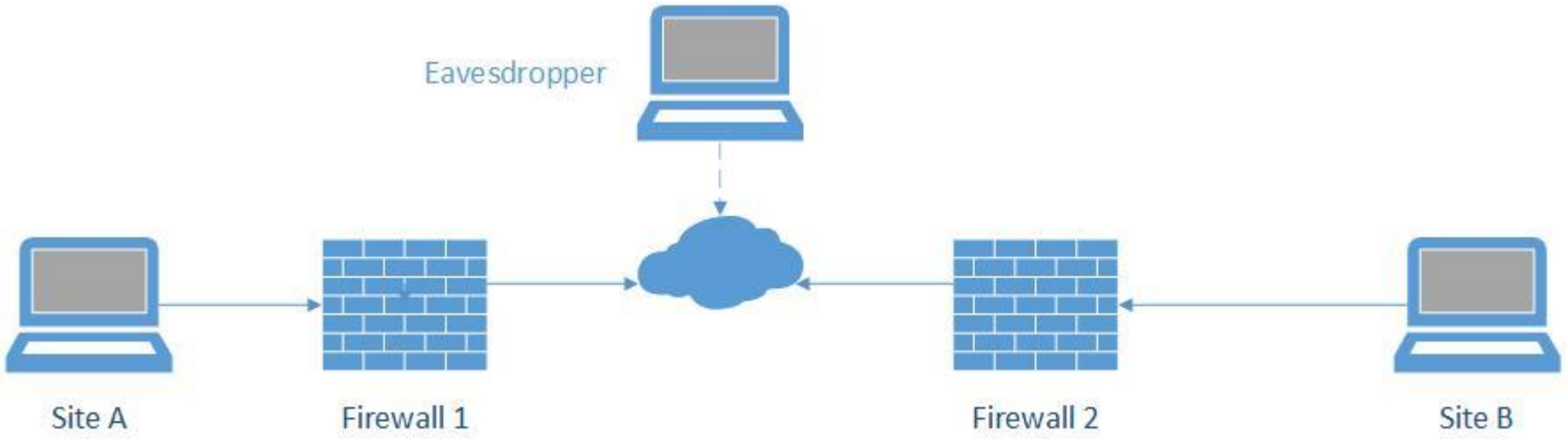
- Secure, encrypted, and private data transmission is important when connecting between two separate sites

- Virtual Private Networks or VPNs are used to achieve this
  - IPSec Protocol is one method for making site-to-site VPNs

- The Office of Naval Research and Integrated Information Technology's project is the framework for why this project is being conducted
  - Creating coursework to train the next generation of cyber security professionals

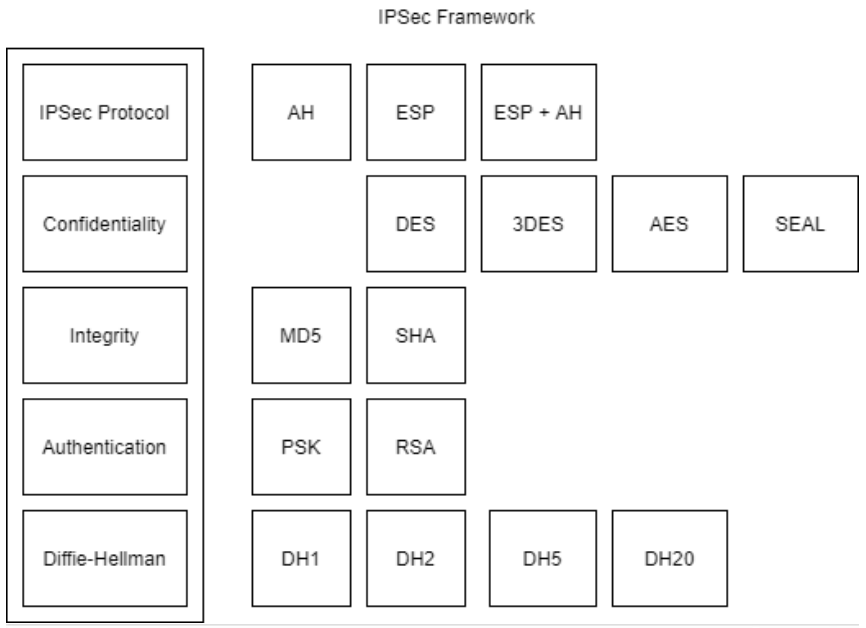
Problem Description

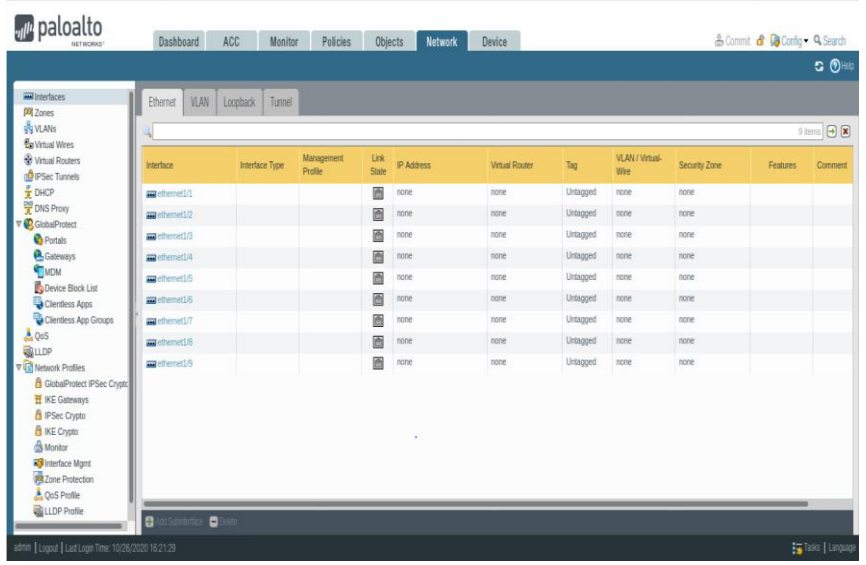
- Connecting two sites to one another directly is a common practice
- Data transmission between two sites needs to be secure, encrypted, and private
- Configuring a functioning Virtual Private Network with the IPSec Protocol
- Testing the Virtual Private Network utilizing the IPSec Protocol



Background Information

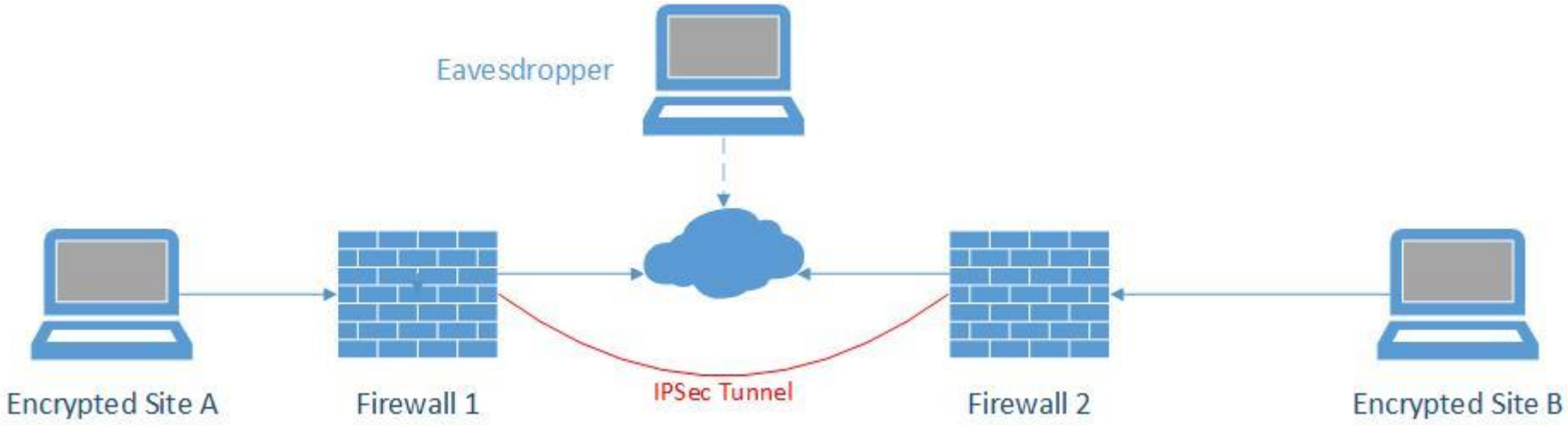
- Next-Generation Firewalls (NGFWs)
- IPSec Protocol components
- IPSec VPN Testing





Proposed Solution and Implementation

- Develop a VPN using IPSec to connect two sites to one another through an IPSec tunnel
- Utilize IPSec components to configure the tunnel
- Develop a lab manual with the concept and configuration of the IPSec tunnel and testing its effectiveness.



Conclusion

- Why is this work important?
- Future projects/concepts with this knowledge
- Questions?