Security Engineering: Secure Networks

Switch Security

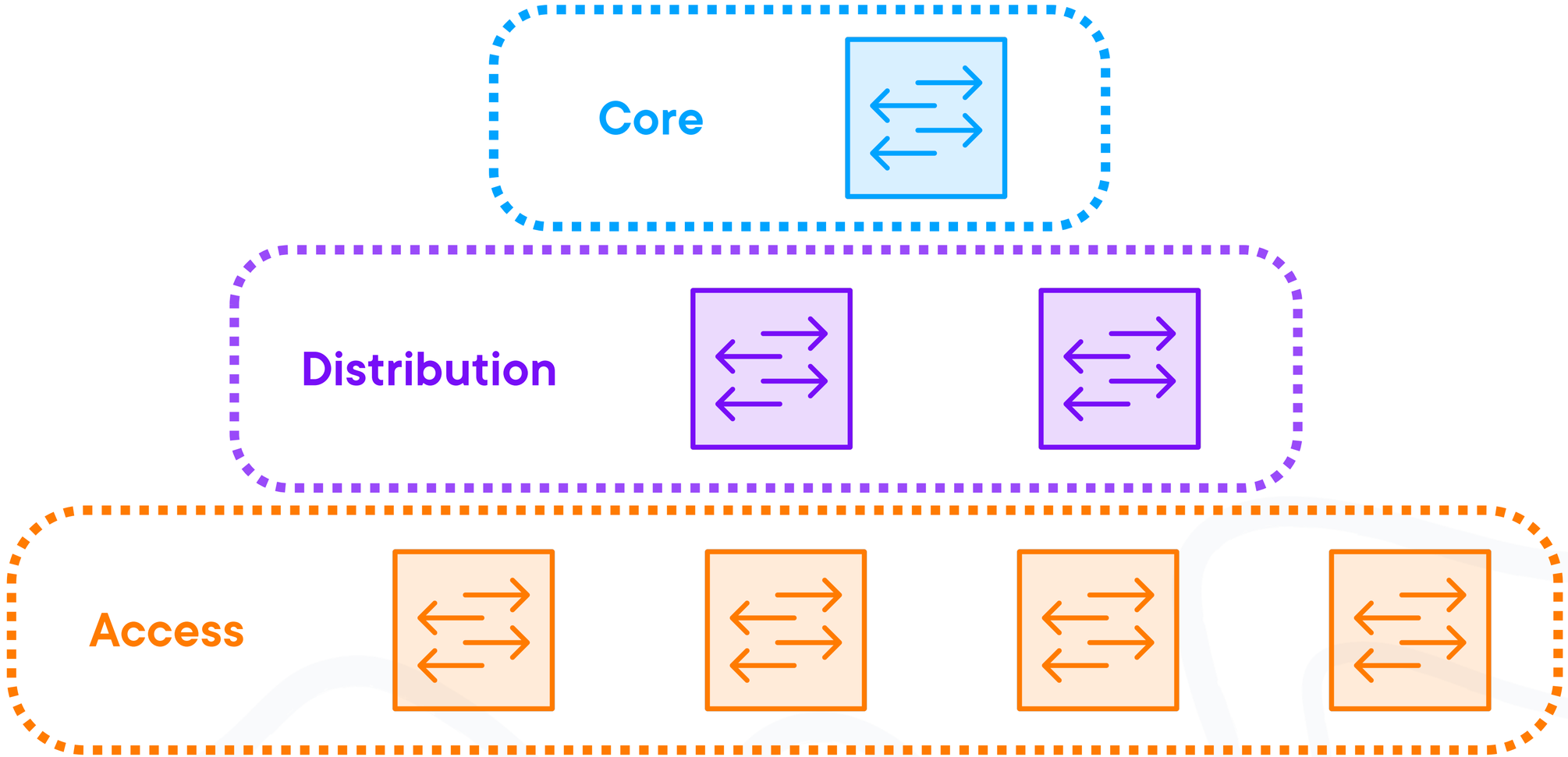


Chris Jackson

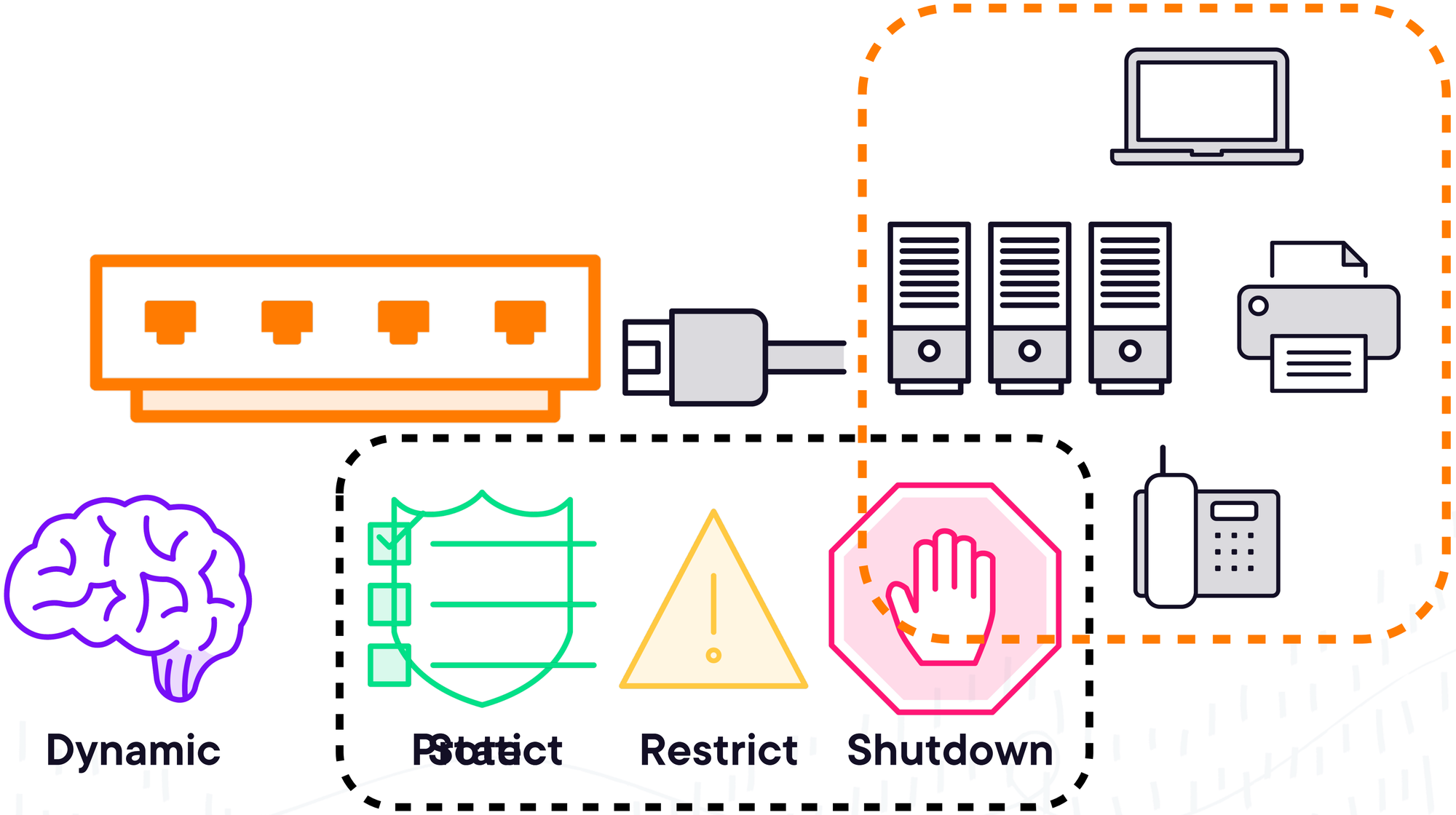
Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

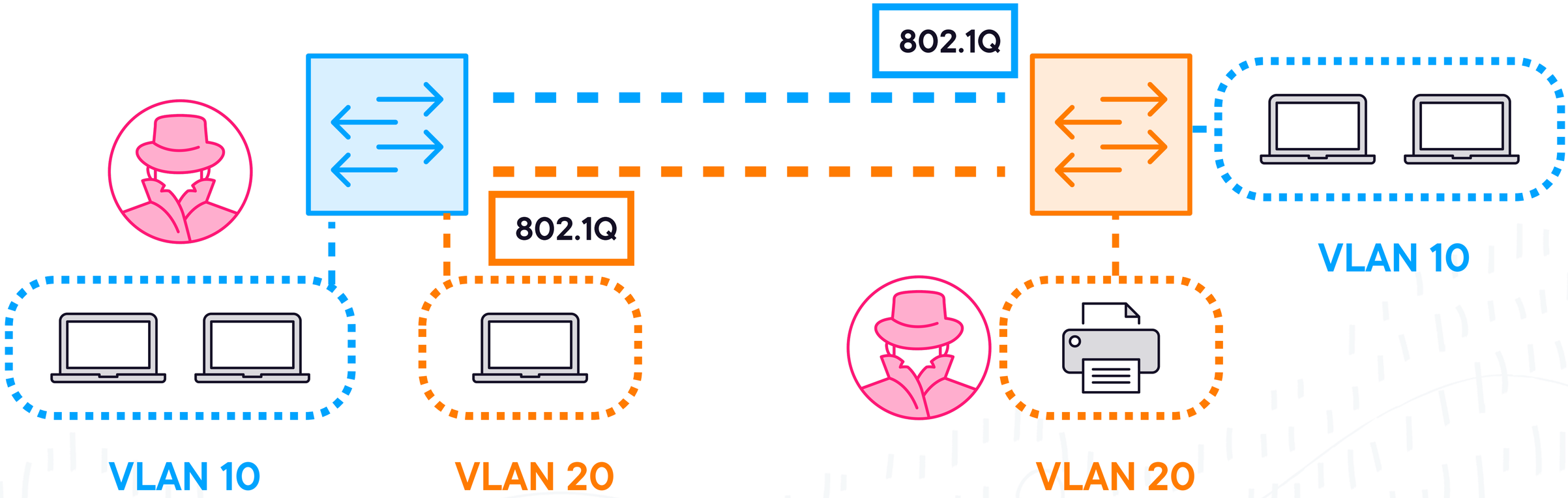
Switch Architecture



Port Security



Virtual Local Area Network (VLAN)



Private VLANs

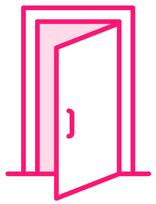


Isolated

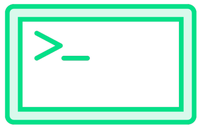


Community

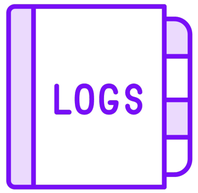
More Switch Security Considerations



Physical Access



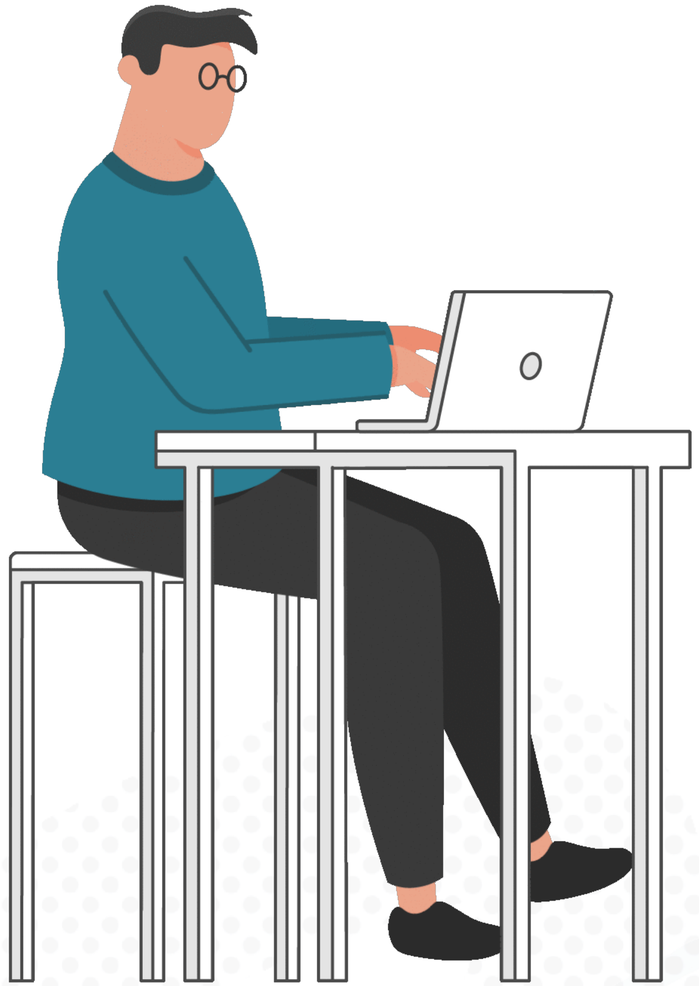
Secure Management Protocols



Enable Logging



Patch Management



Router Security

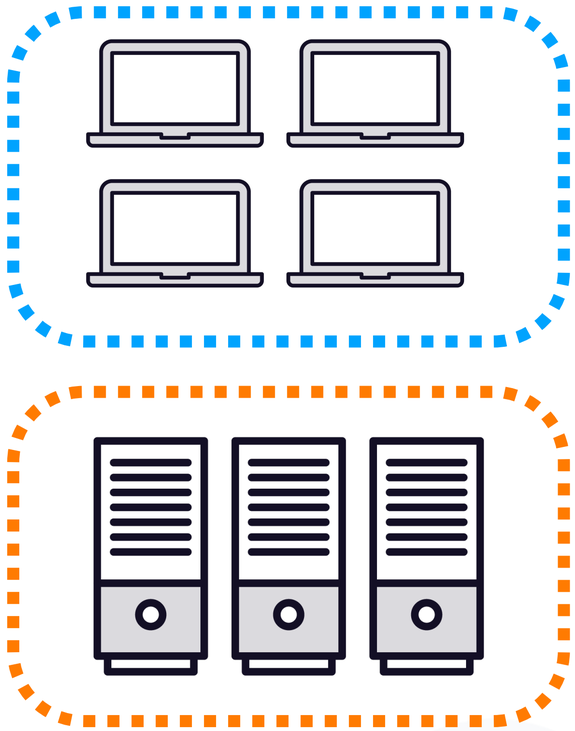


Chris Jackson

Pluralsight Author

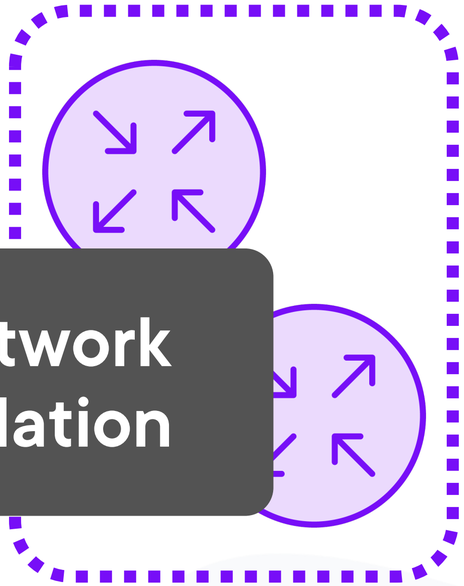
ChrisJacksonMSIT | CyberTitanLLC.com

Subnets



10.0.50.0 /24

10.0.20.0 /27



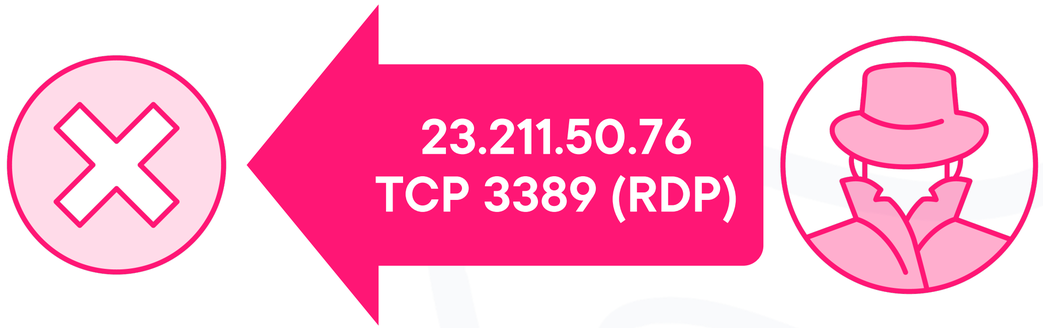
/30

Access Control Lists (ACLs)

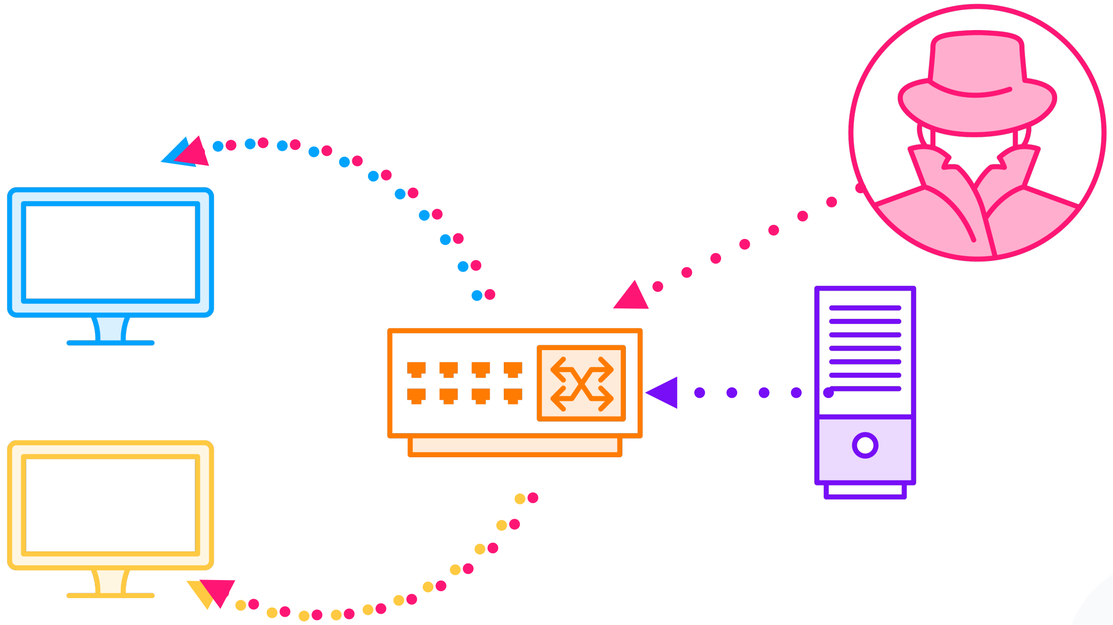








Network Address Translation (NAT)



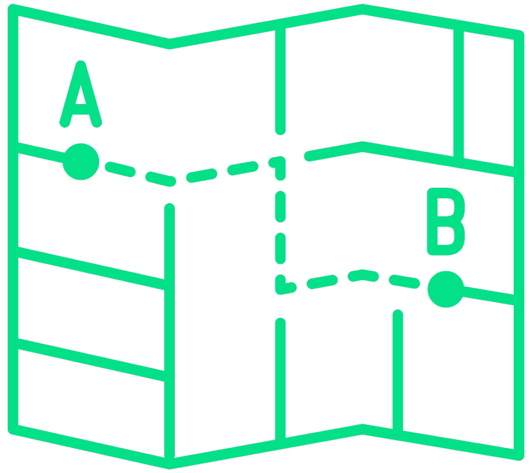
Port Forwarding

Network Address Translation (NAT)

Compatibility Issues

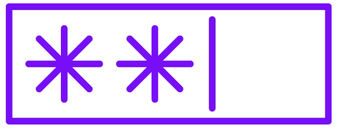


Network Address Translation (NAT)



NAT Traversal

Securing Routing Protocols



AuthN

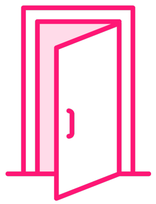


TTL

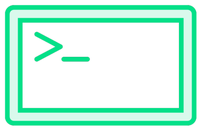


Filtering

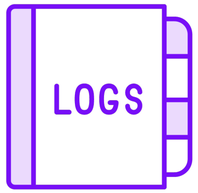
More Router Security Considerations



Physical Access



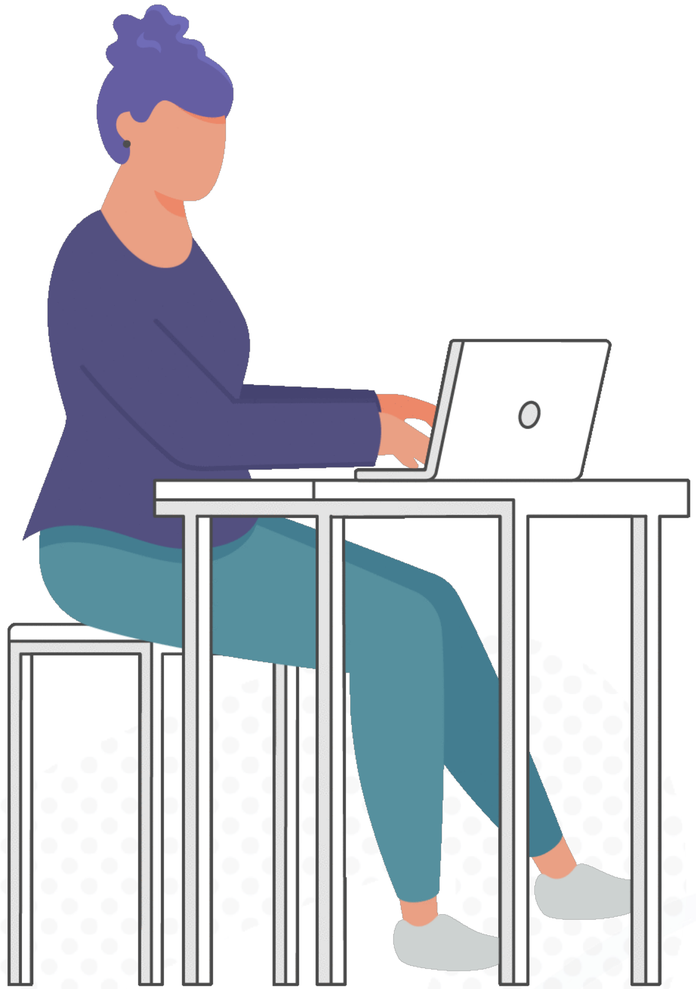
Secure Management Protocols



Enable Logging



Patch Management



Wireless Network Security



Chris Jackson

Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

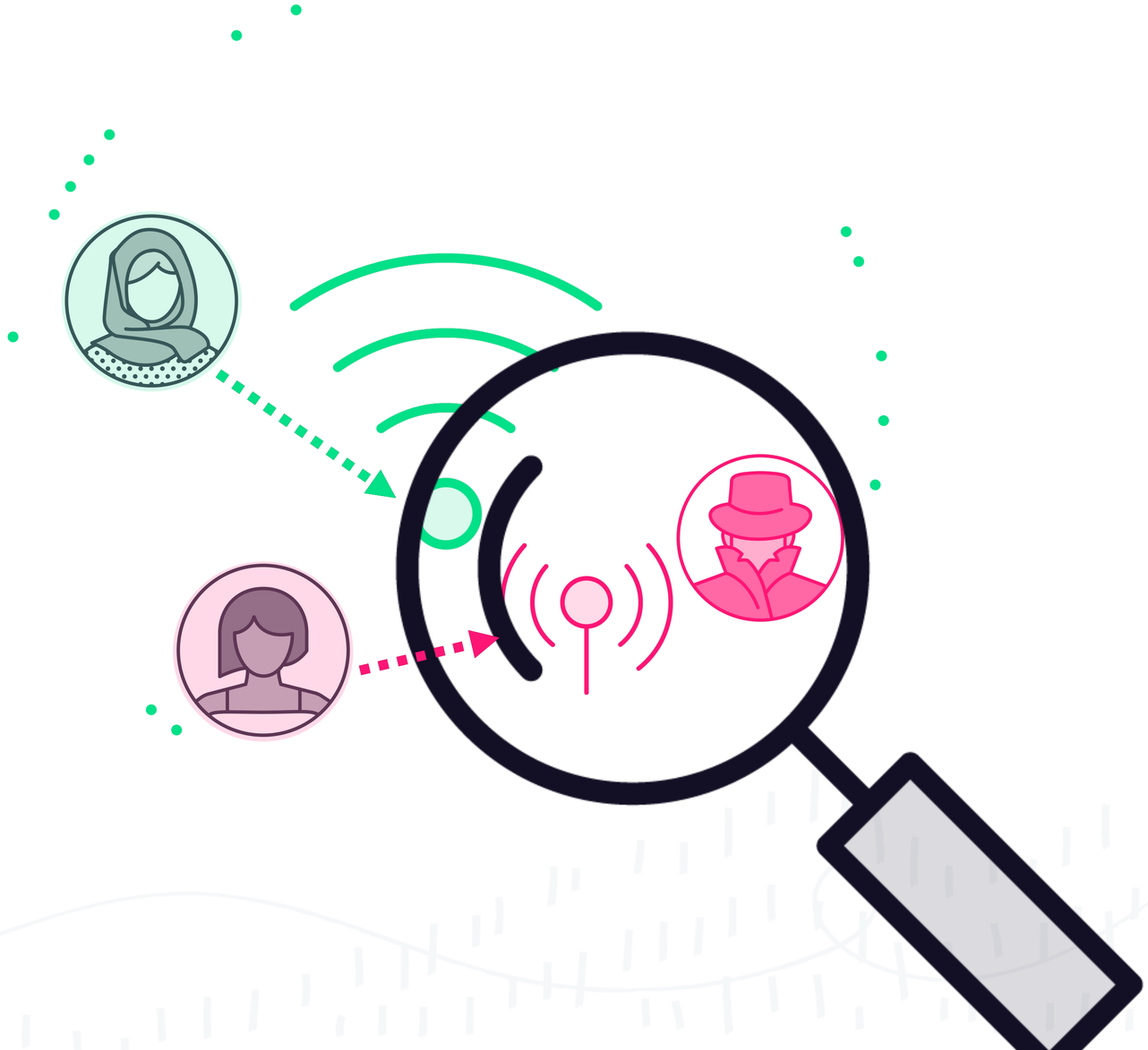
Wireless Technologies



Signal Security



Rouge Access Points



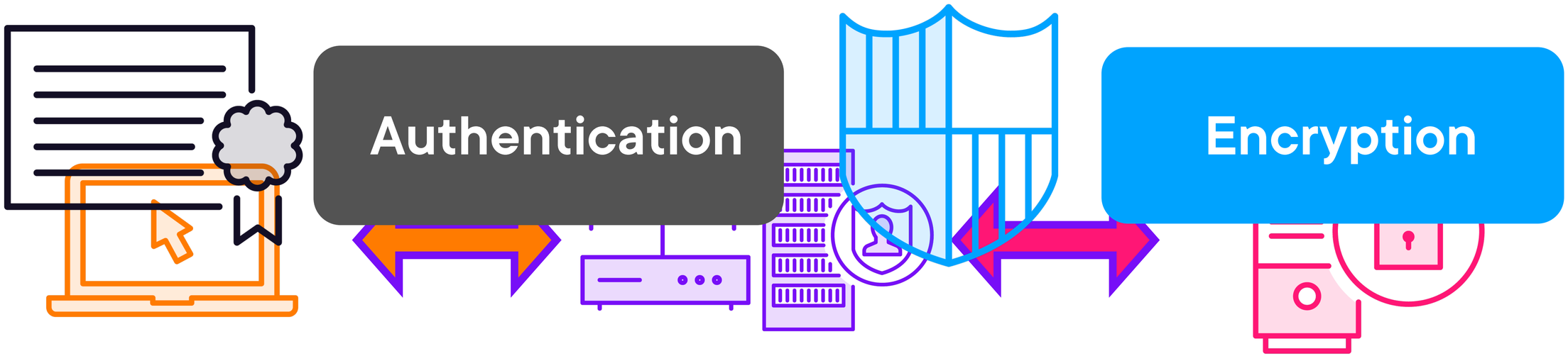
Guest Security







Wireless Connection Security



Supplicant

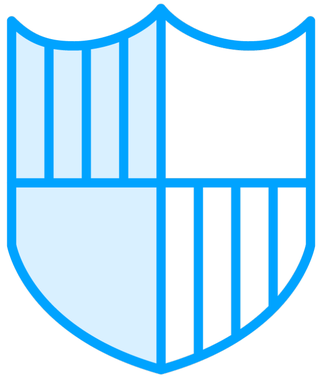
Authenticato
r

Authentication
Server

Wireless Connection Security



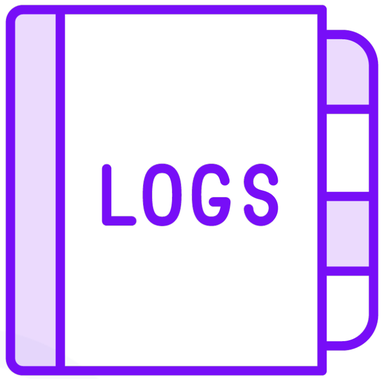
Authentication



Encryption



Patch and Harden



Logging

Virtual Private Network (VPN)



Chris Jackson

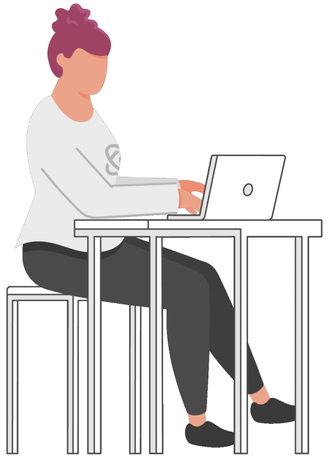
Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

Site-to-Site



Remote-to-Site



Atlanta

0101000001010011



0101000001010011

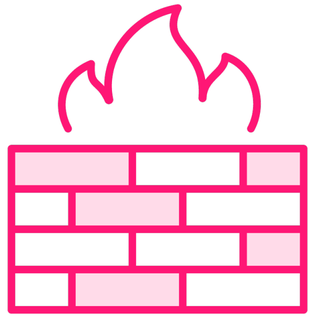


NYC

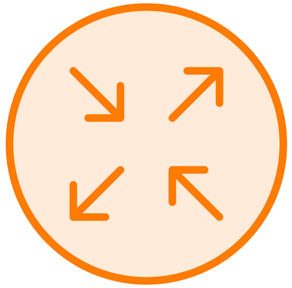
VPN Architecture



VPN Tunnel



Firewall



Router



VPN

Protocols

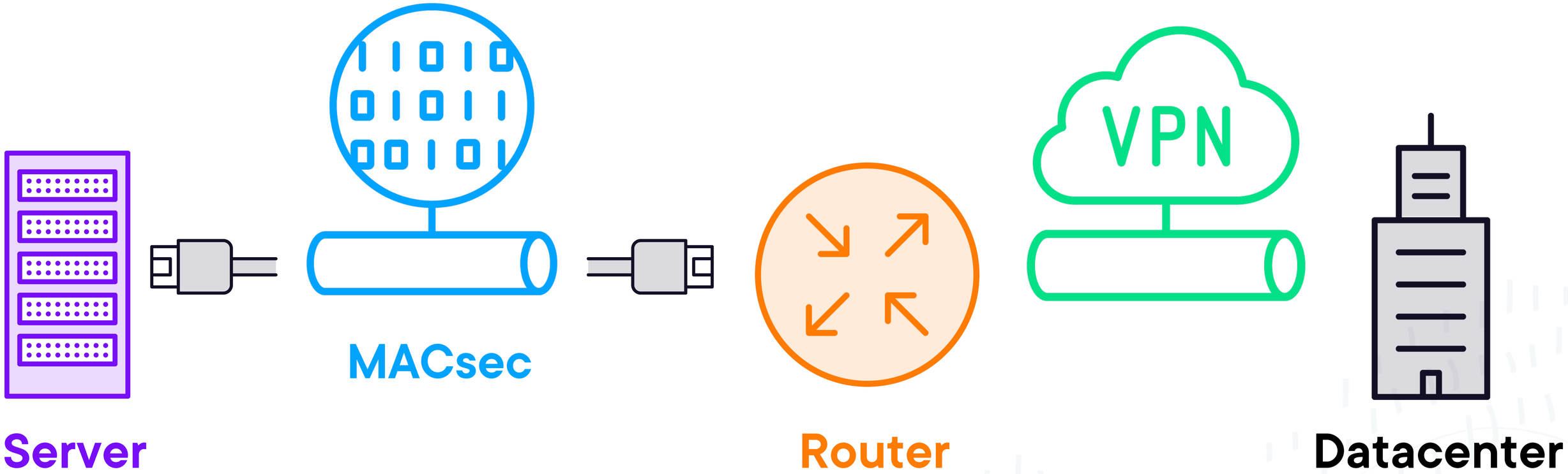
IPsec

- ★ Network Layer
- ★ IKE
- ★ ESP
- ★ AH

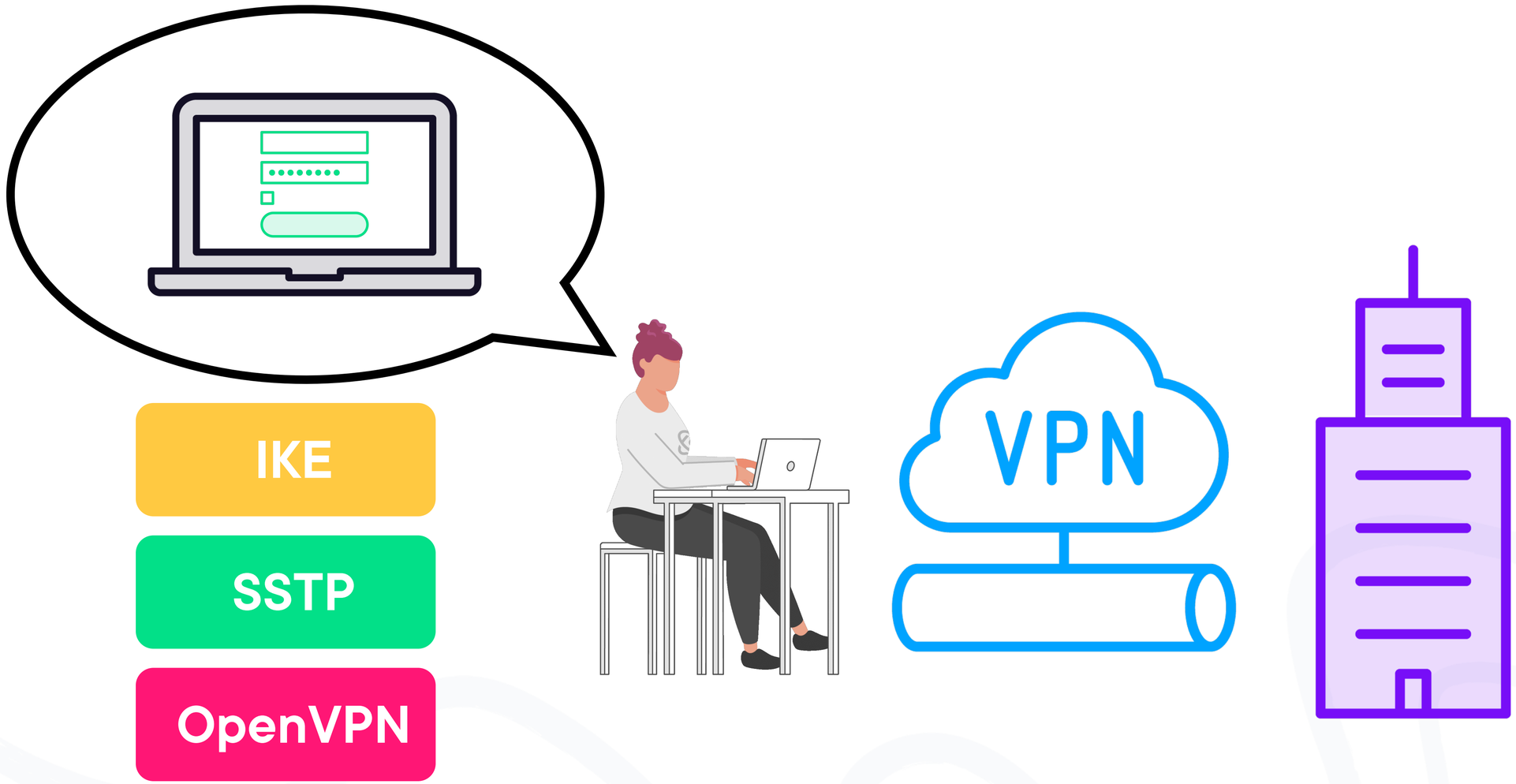
MACsec

- ★ Data-Link Layer
- ★ Confidentiality
- ★ Integrity
- ★ Authenticity

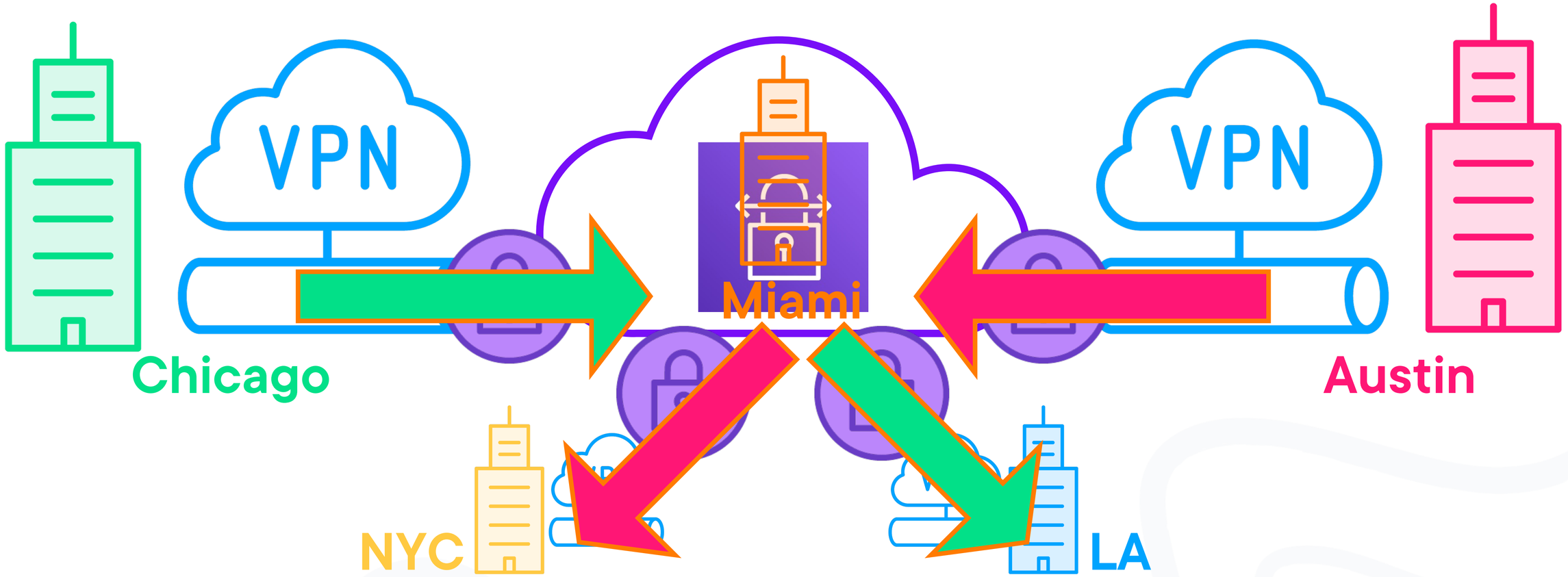
MACsec



Cloud-based VPN



Cloud-based VPN



Logging and Reporting



Chris Jackson

Pluralsight Author

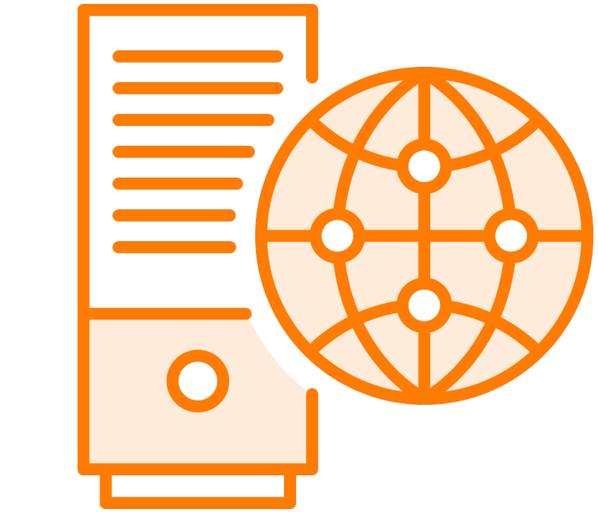
ChrisJacksonMSIT | CyberTitanLLC.com

What's the Purpose of Logging?

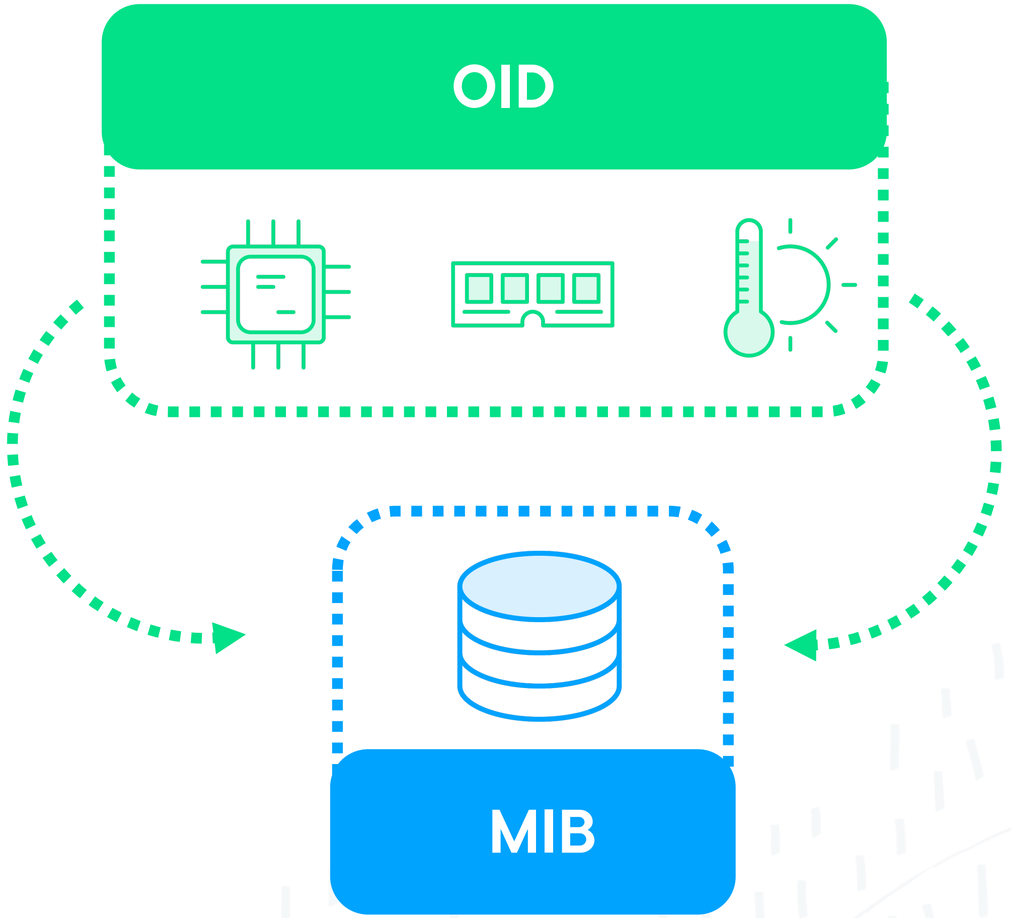


Who What When Where Why

Centralized Network Logging



Simple Network Management Protocol



Centralized Network Logging



SysLog



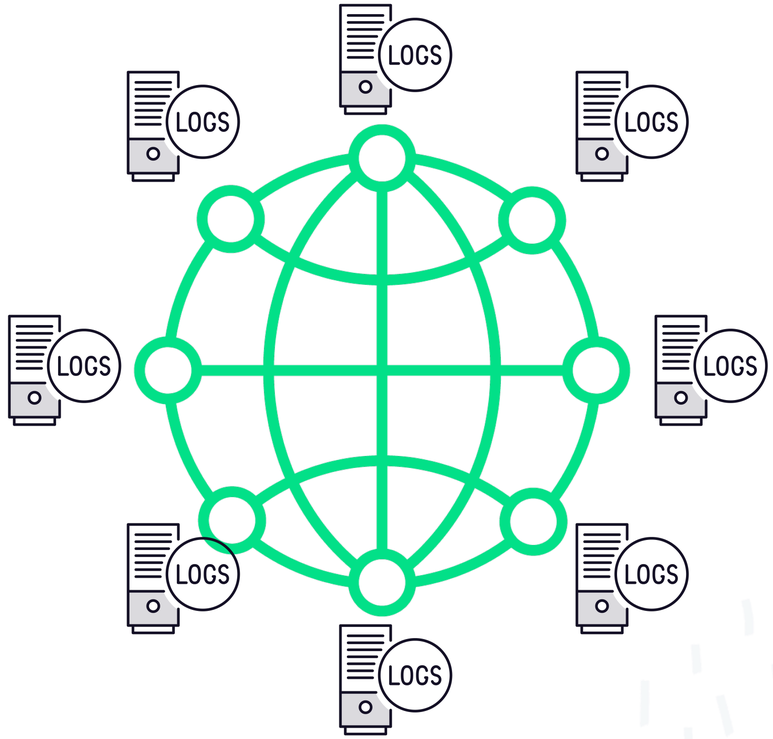
Security Information and Event Management

Centralized Network Logging

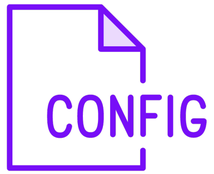


SysLog

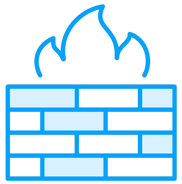




What to Log



Configuration Changes



Access and Protocol Activity

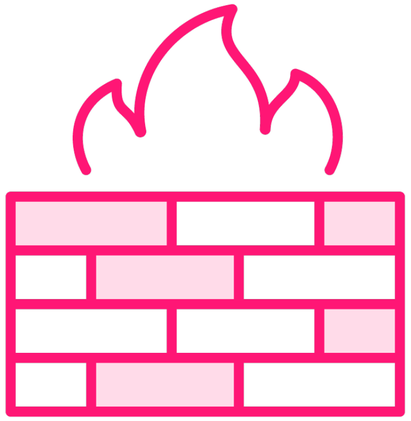


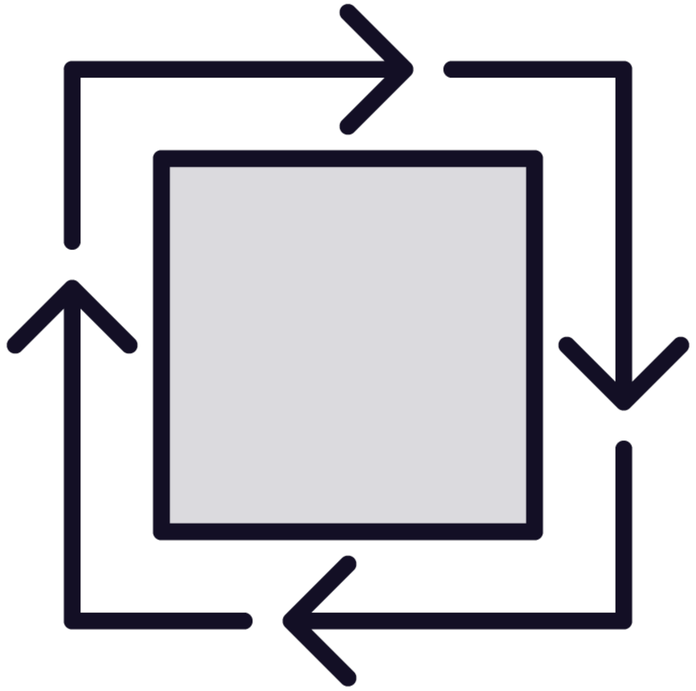
Failed Authentication Attempts

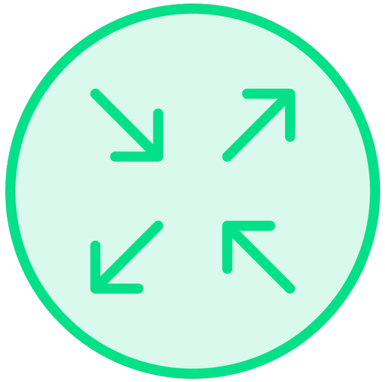


Data Exfiltration

What to Log







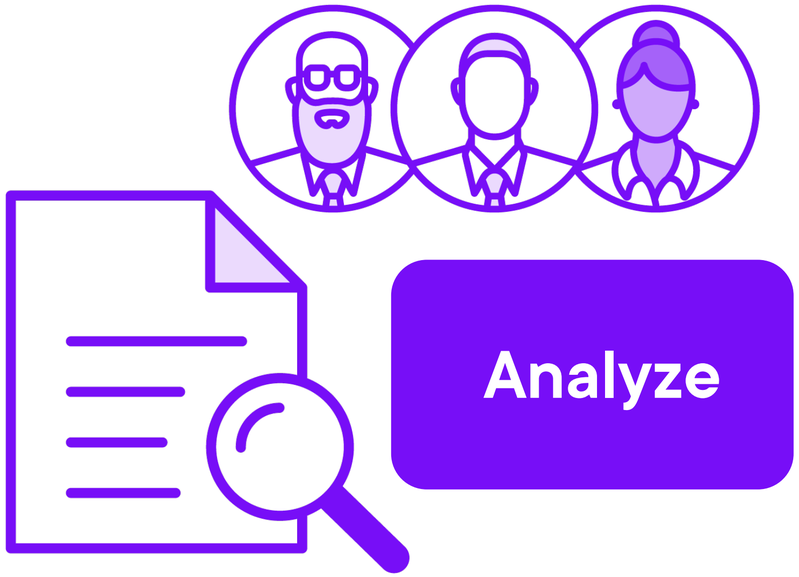
Boundaries and Edge

What to Log



Performance

Dig Deeper





Network Taps

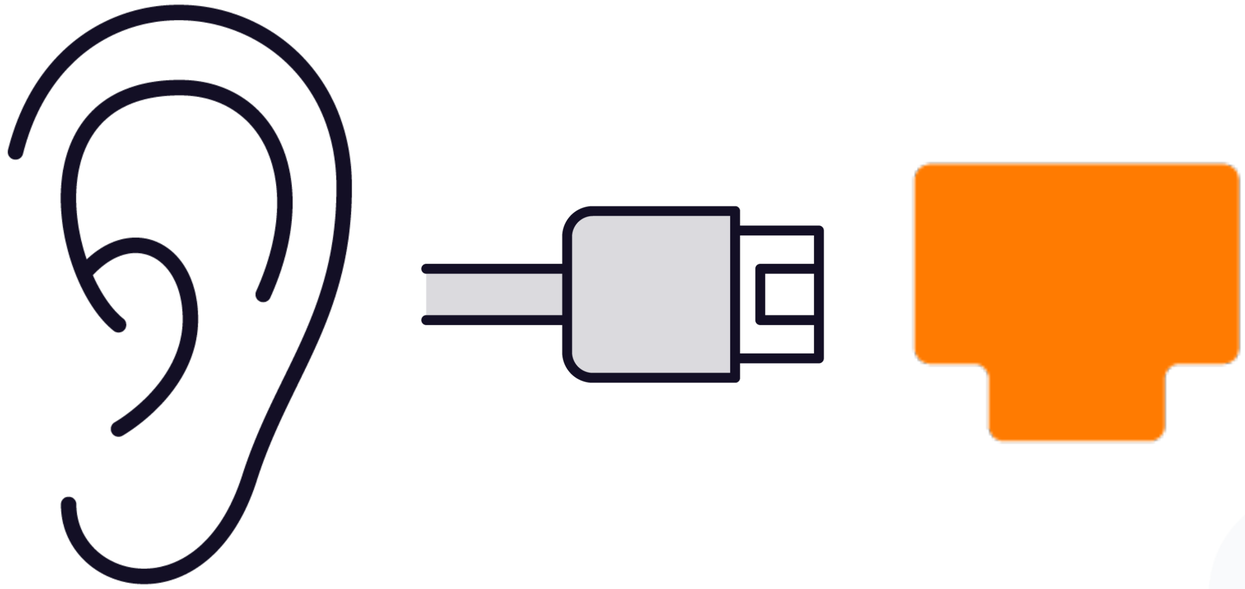


Chris Jackson

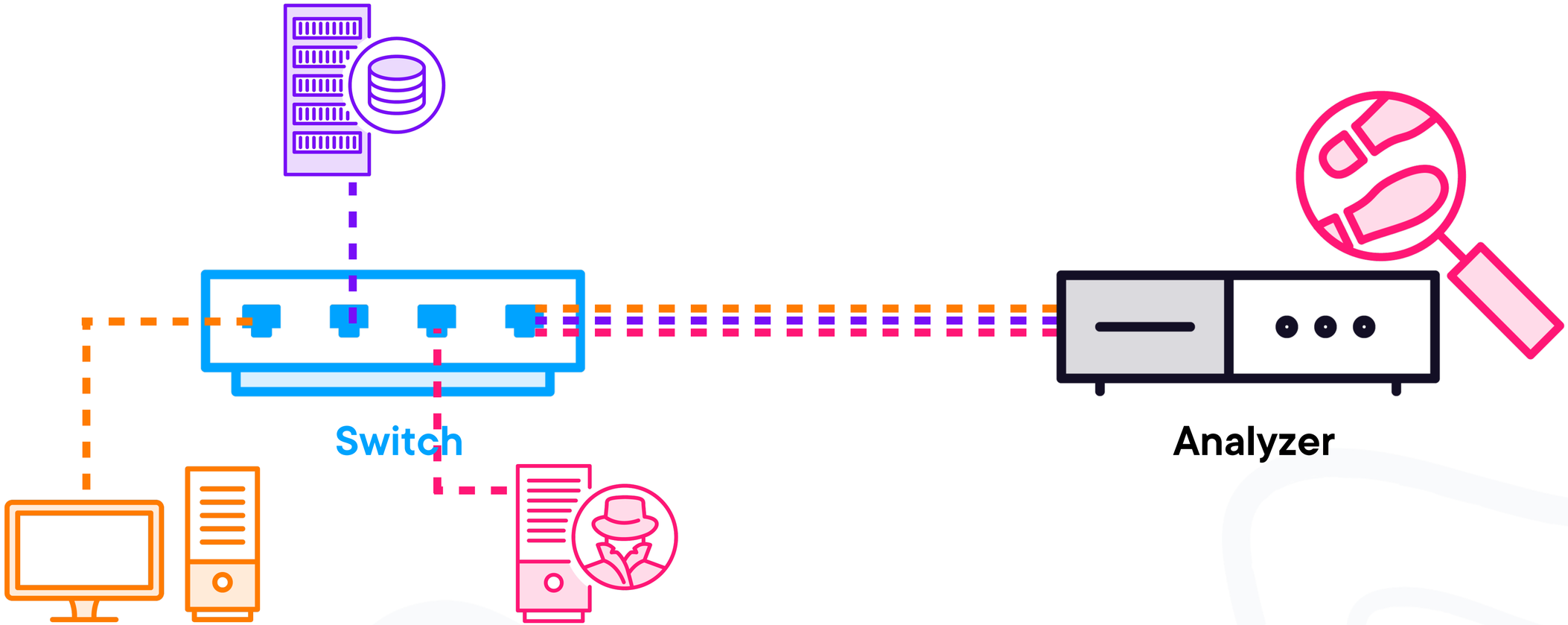
Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

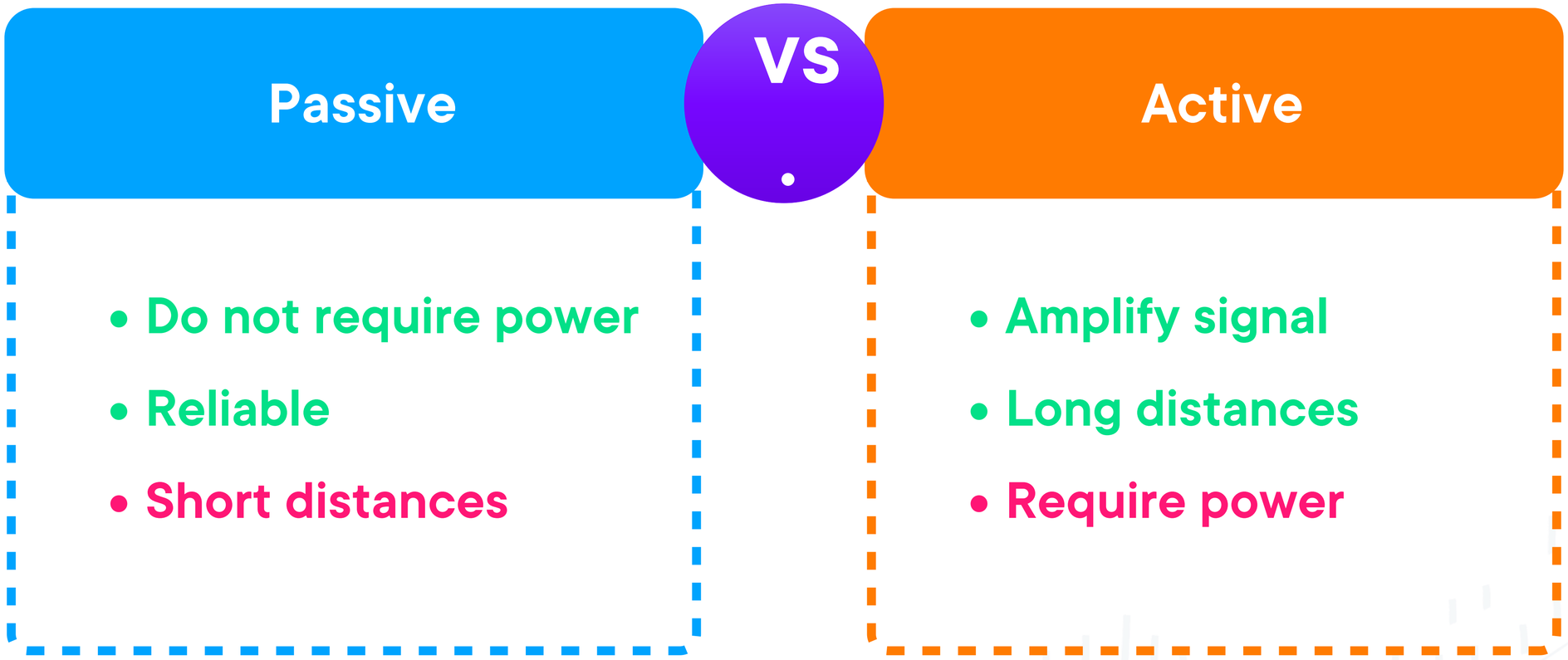
Network Taps



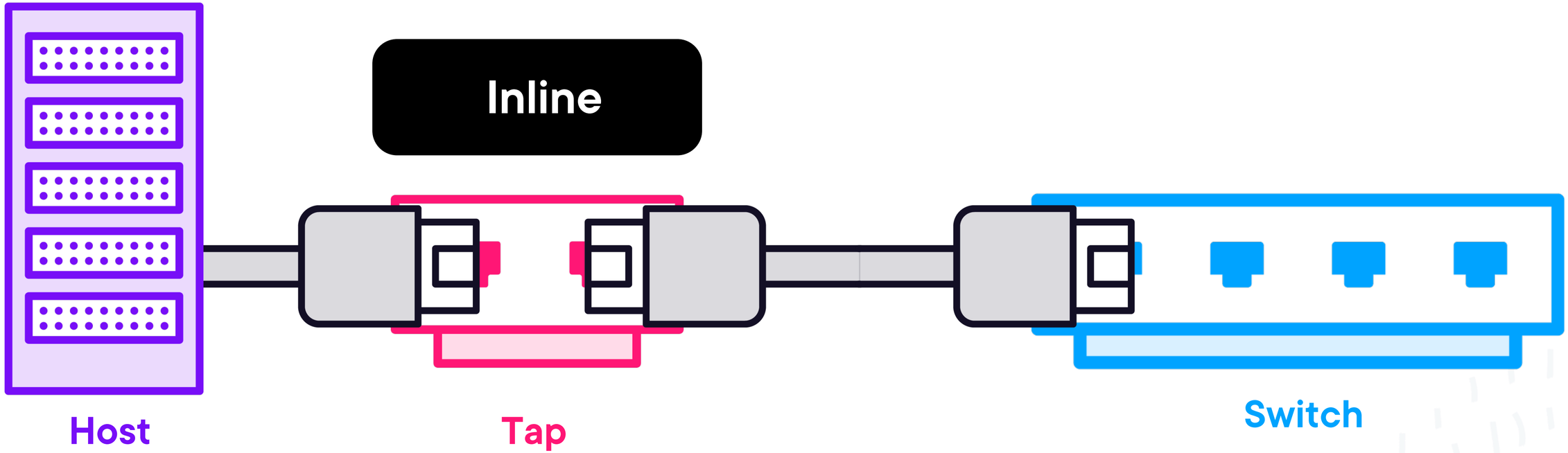
Port Mirroring



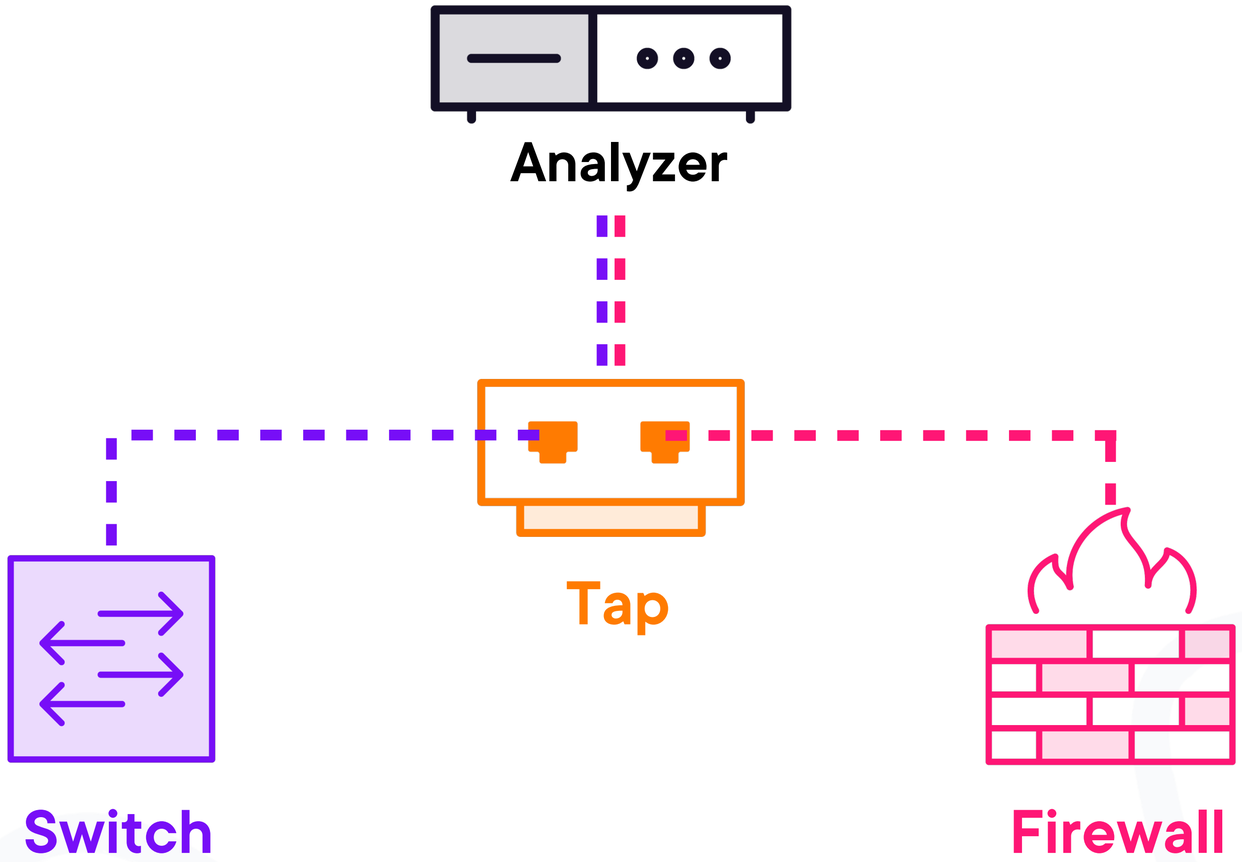
Passive vs. Active



Inline



Aggregator



Regeneration

