Proxies

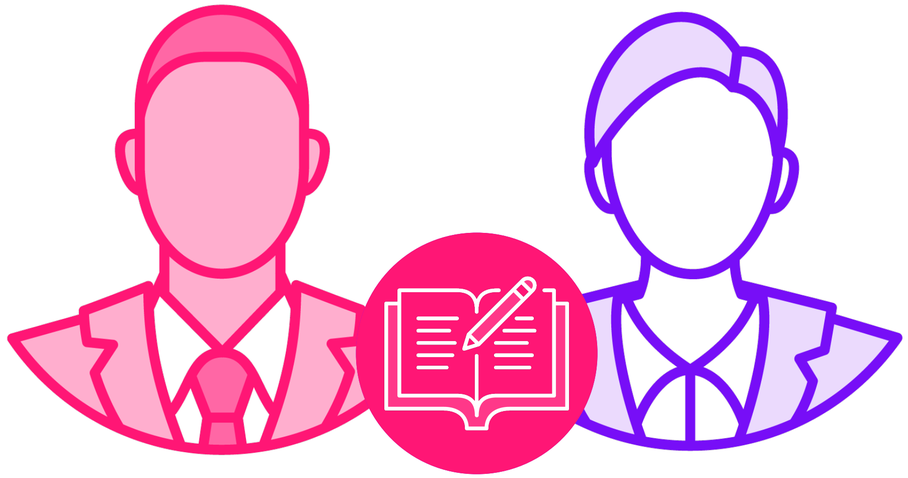


Chris Jackson

Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

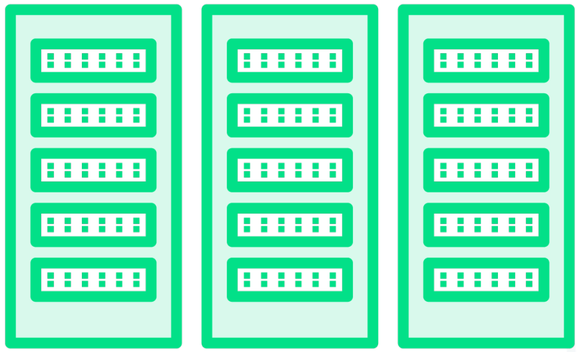
What are Proxies?



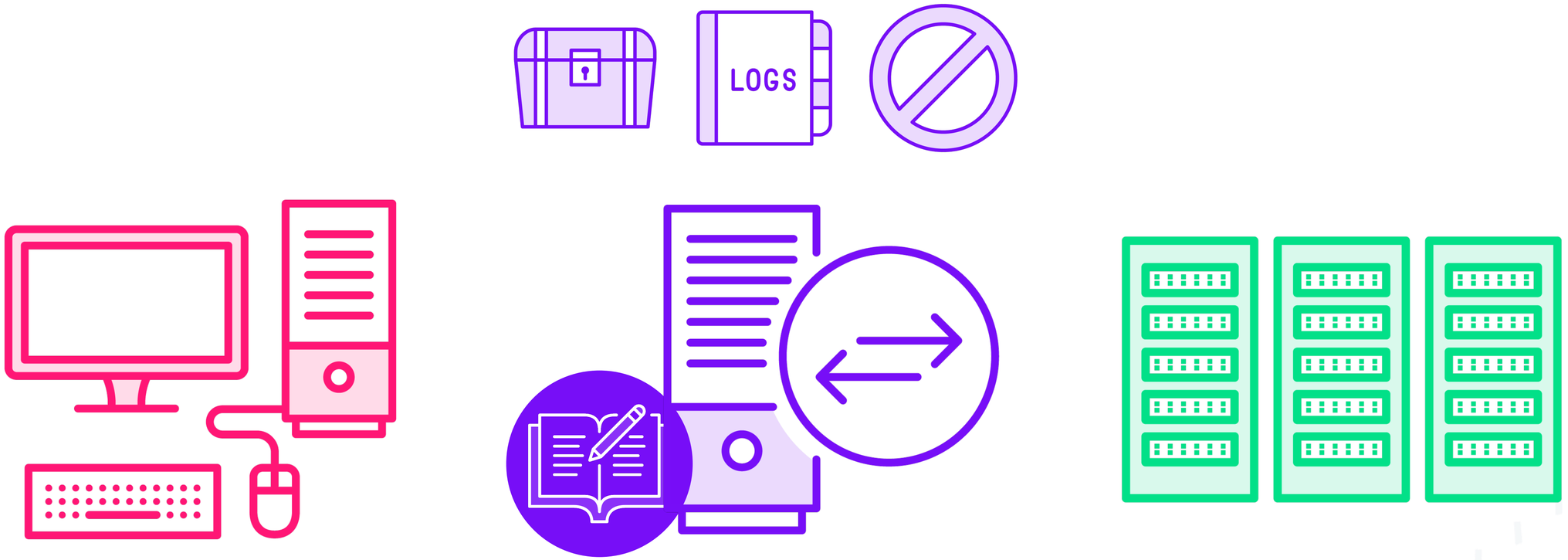


Forward Proxy

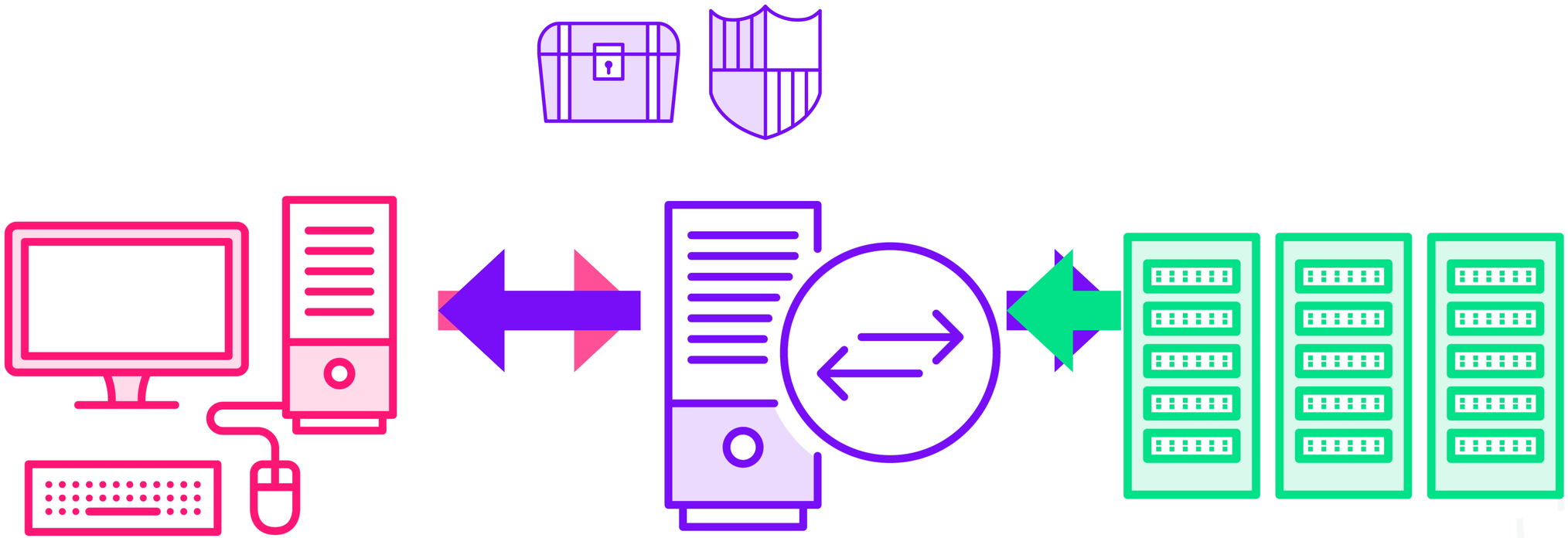




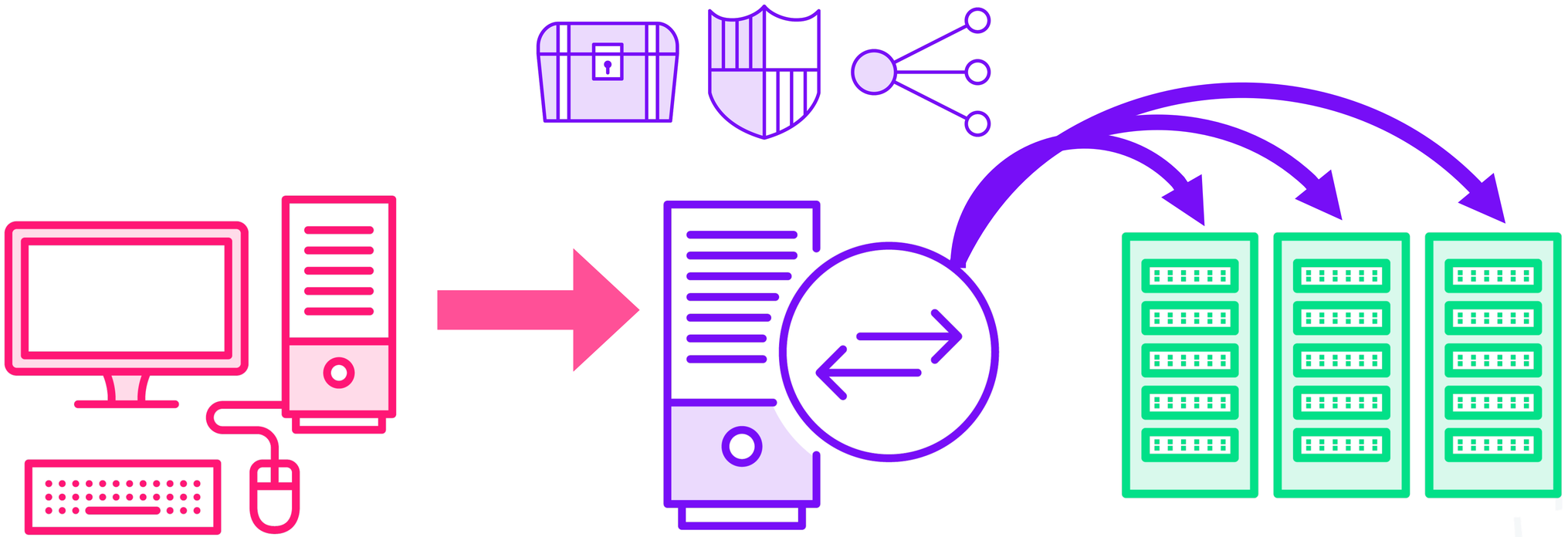
Forward Proxy



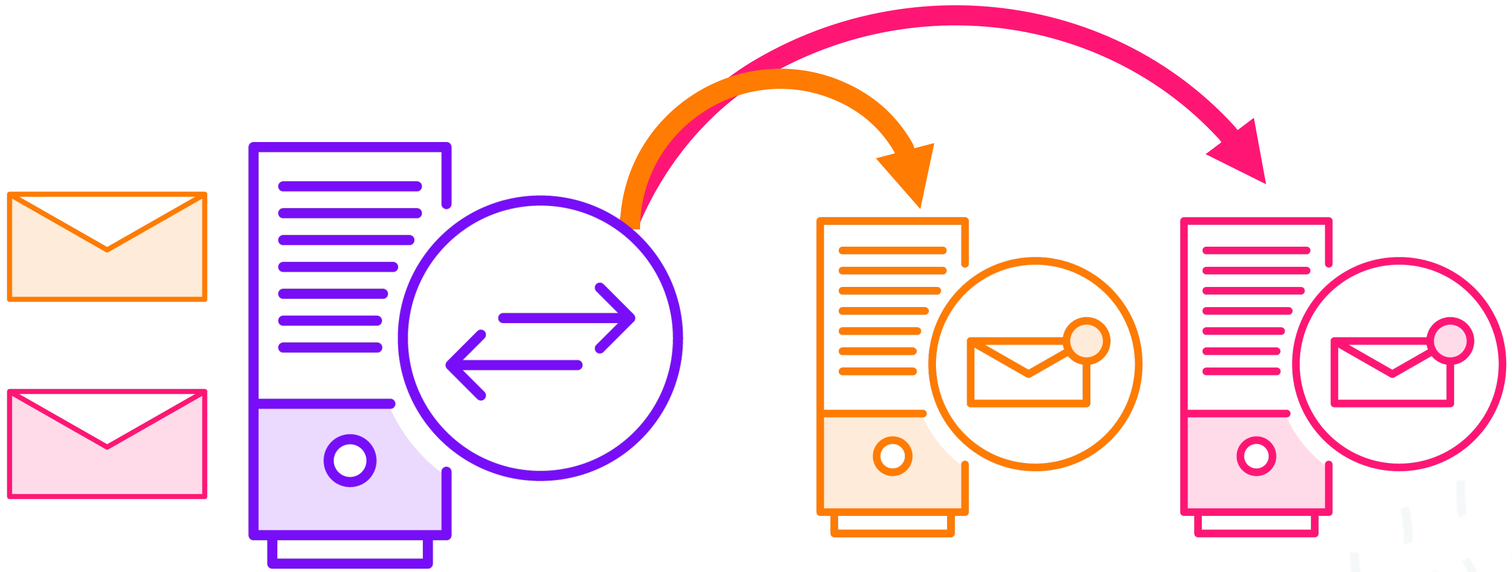
Reverse Proxy



Reverse Proxy



SMTP Proxy



Tiered Architecture

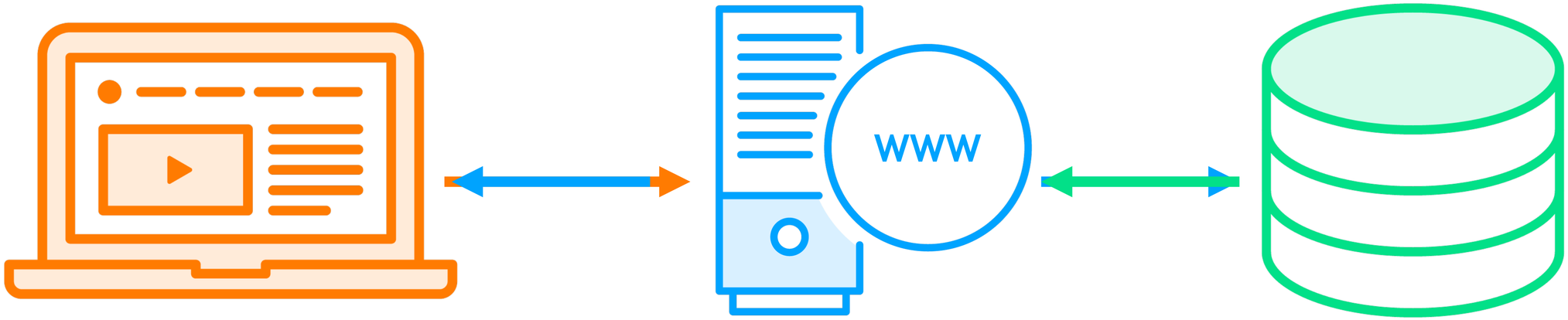


Chris Jackson

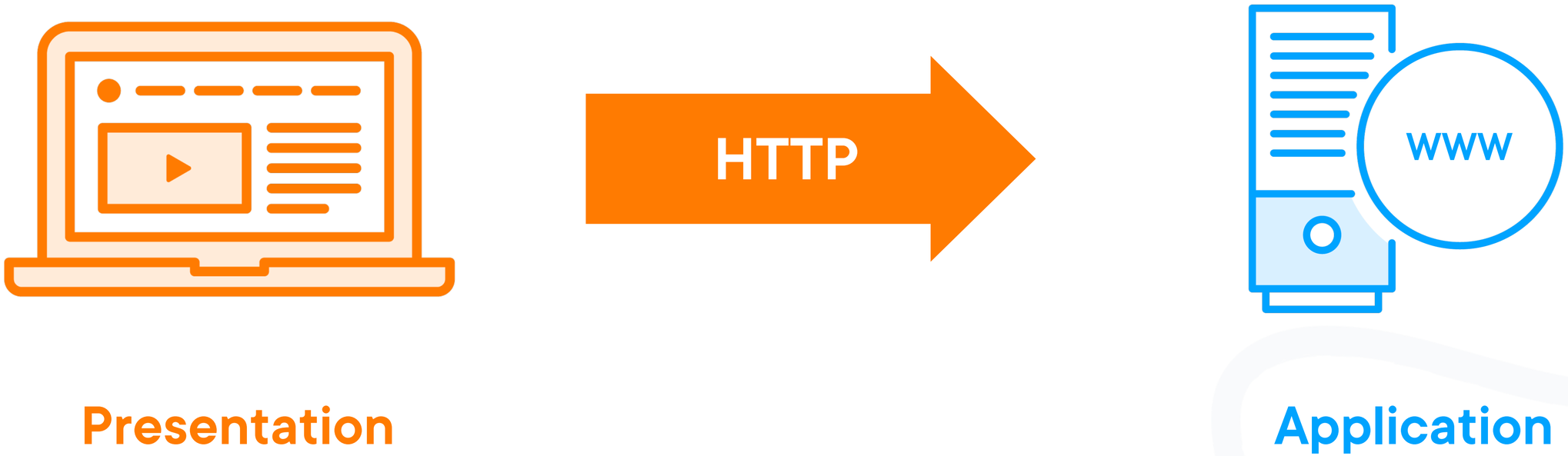
Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

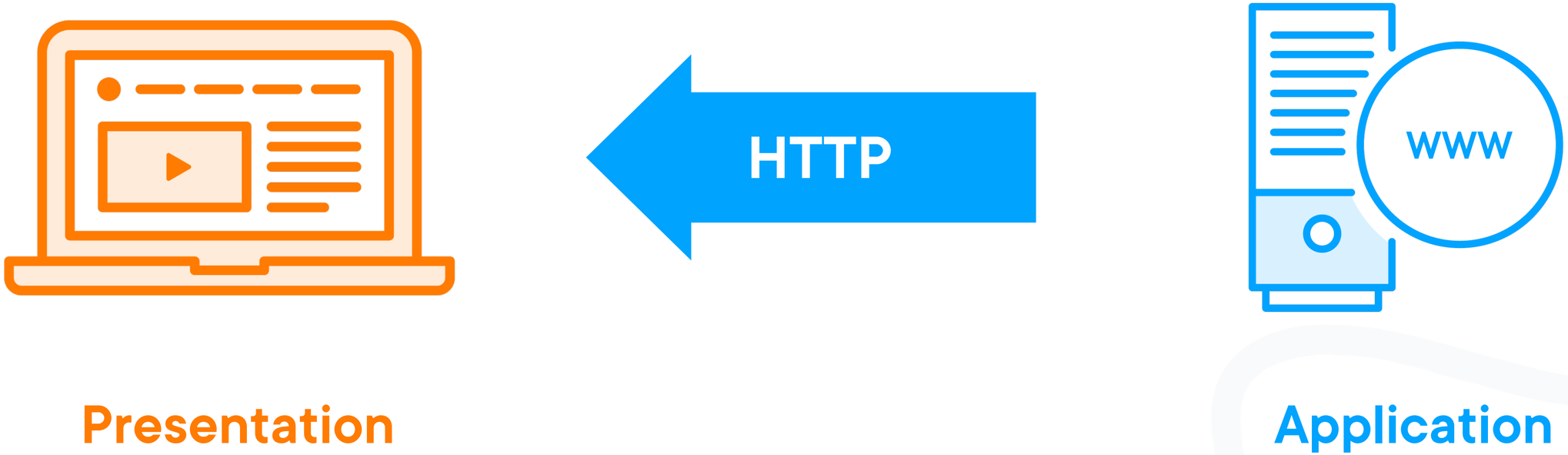
Tiered Architecture



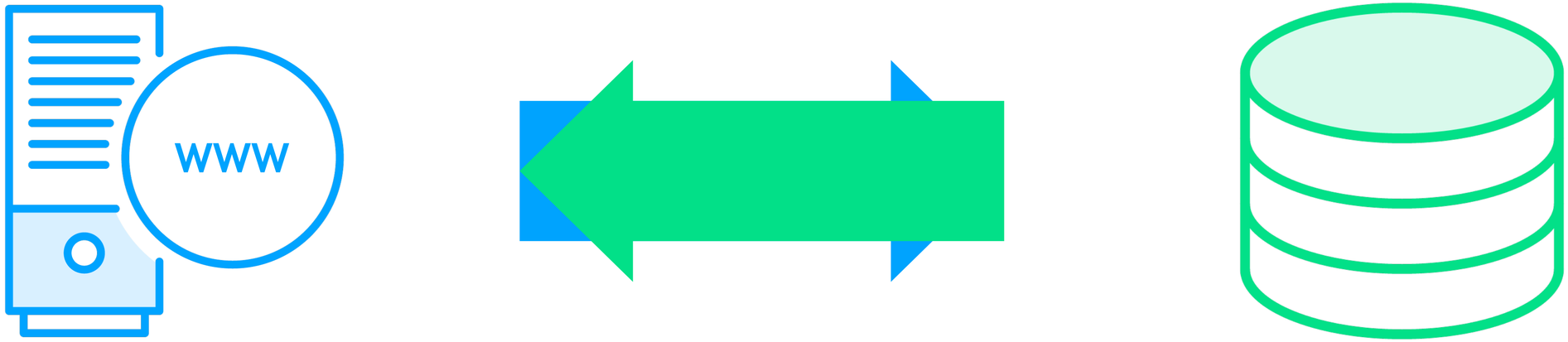
Tiered Architecture



Tiered Architecture



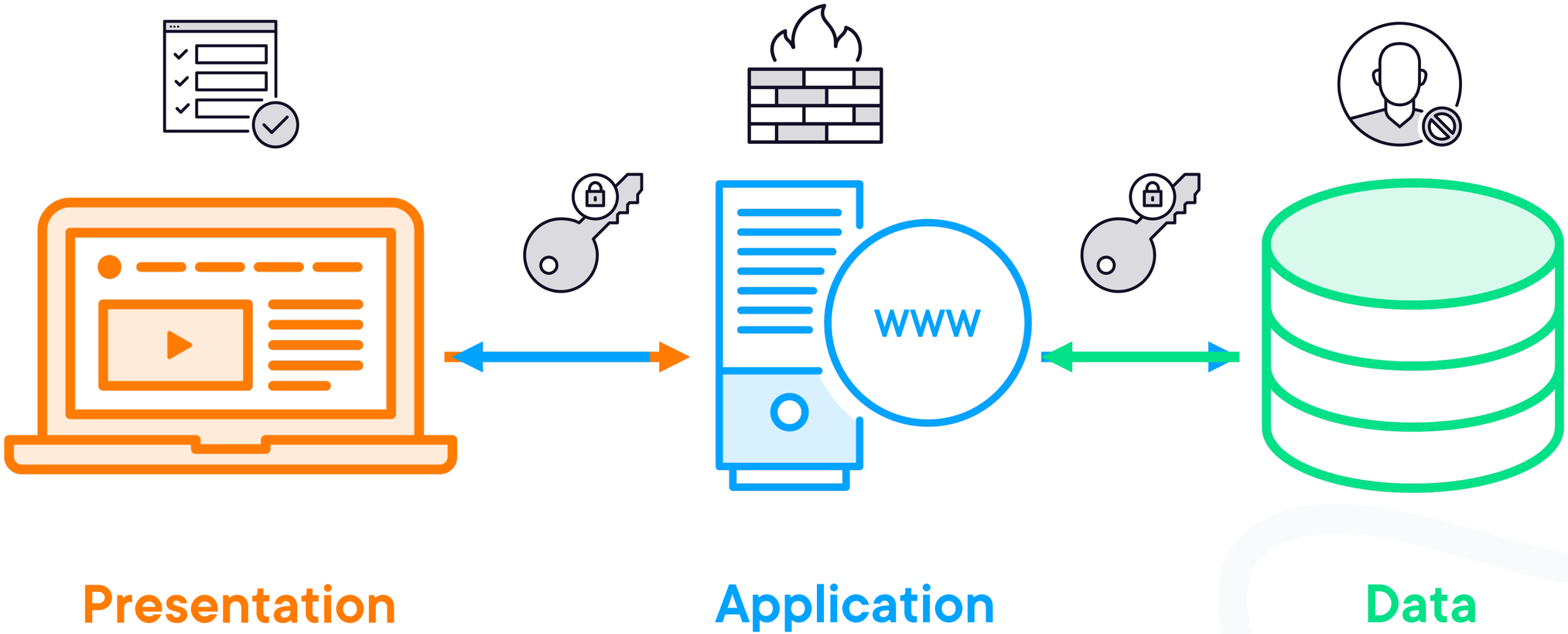
Tiered Architecture



Application

Data

Tiered Architecture



Firewalls

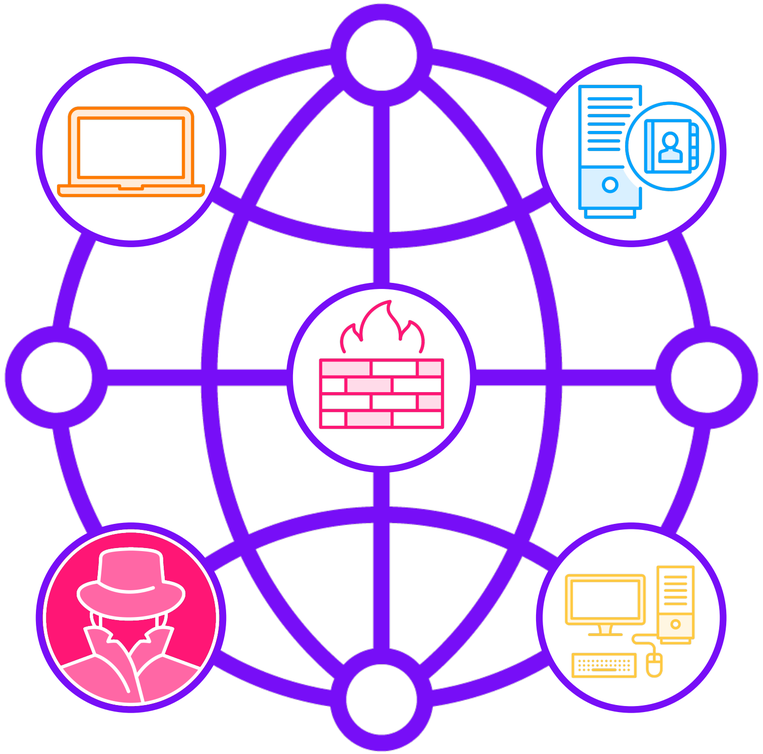


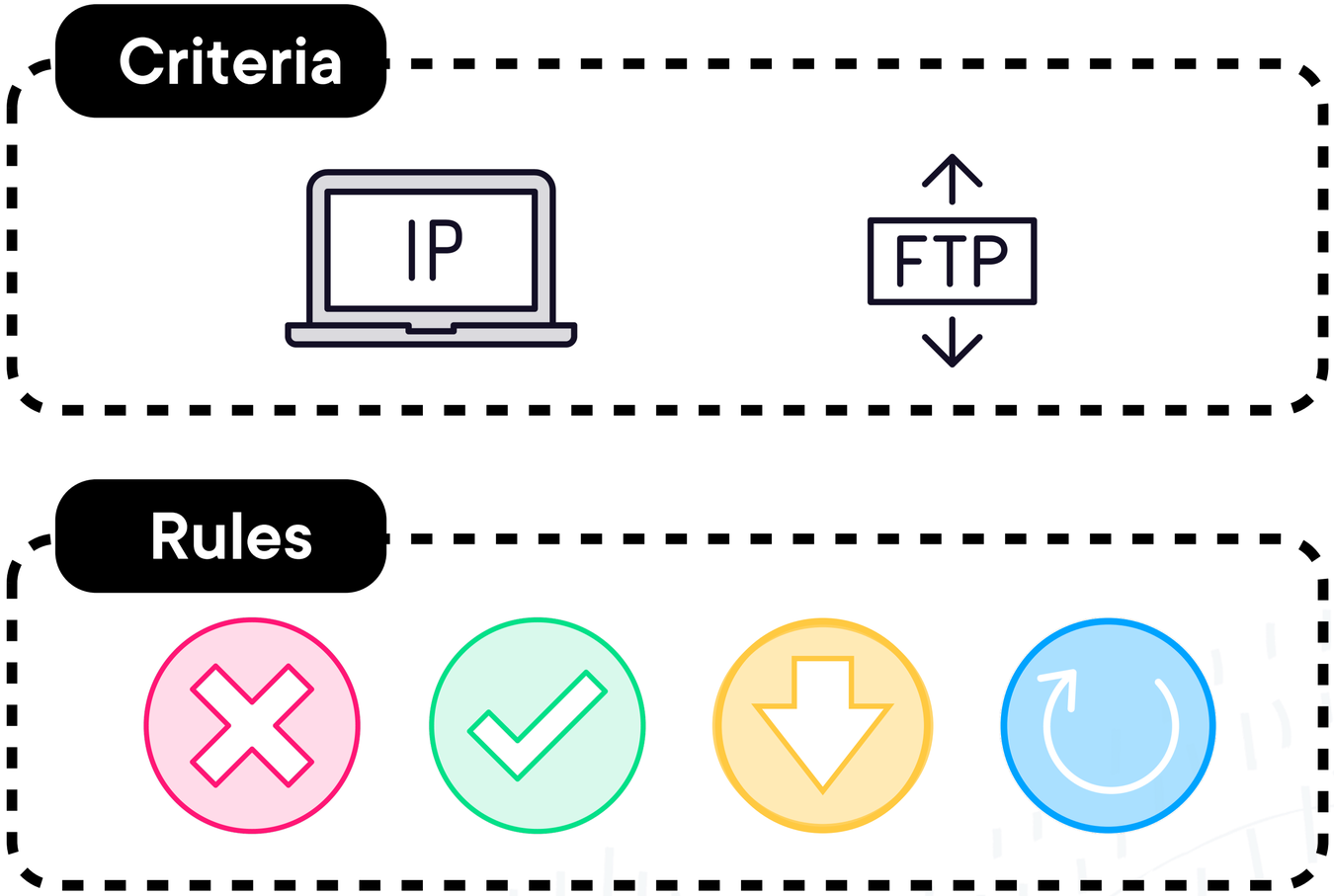
Chris Jackson

Pluralsight Author

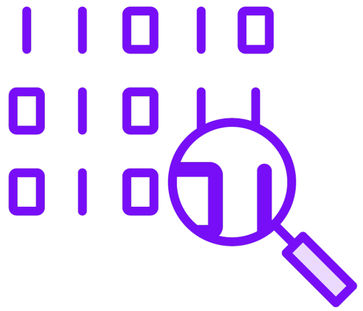
ChrisJacksonMSIT | CyberTitanLLC.com

Network Firewalls

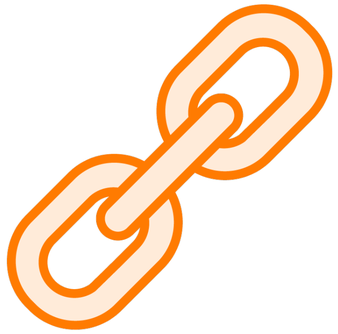




Next Generation Firewall (NGFW)



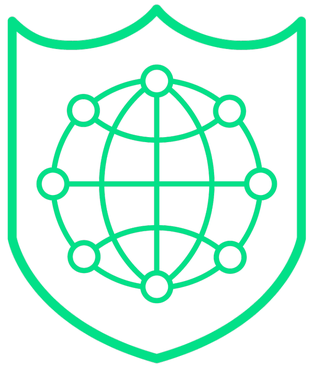
Inspection



Stateful

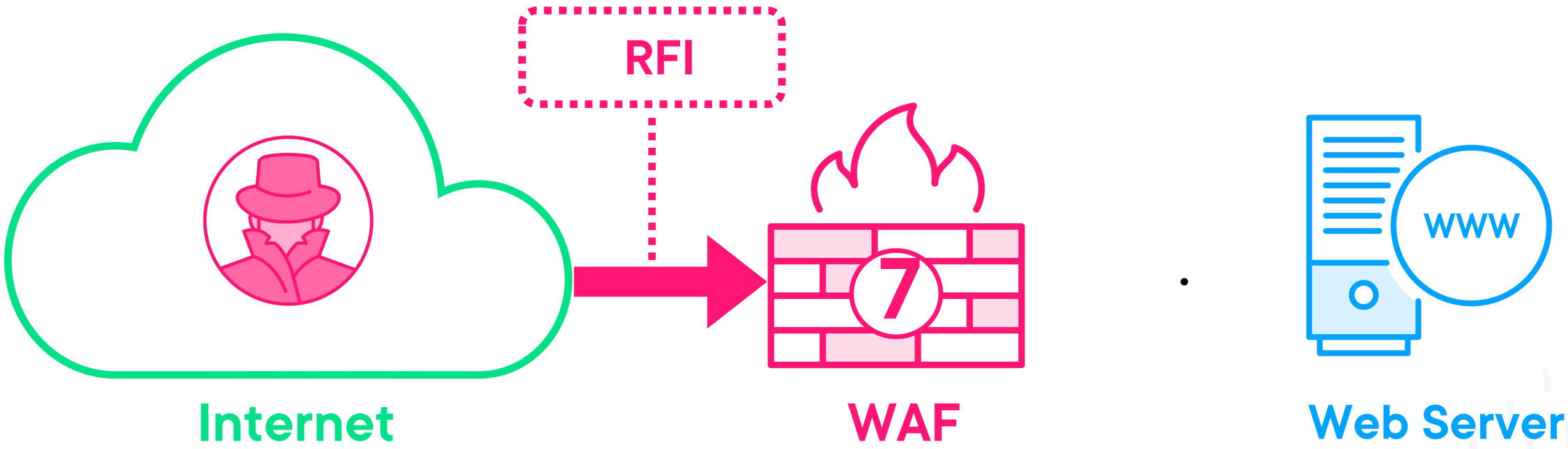


Threat Intel

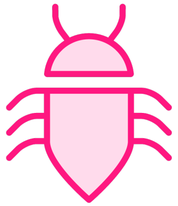


Detection and Prevention

Web Application Firewall (WAF)



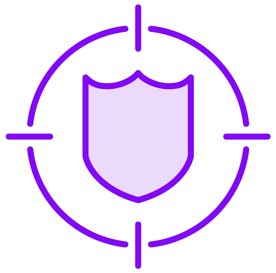
OWASP



OWASP Top 10 is a list of the most notorious web application security risks and vulnerabilities, which includes SQLi, XSS, and others.



Open Worldwide Application Security Project (OWASP) is an organization dedicated to studying and publishing lists related to web app security



ModSecurity is an open-source WAF that utilizes the Core Rule Set to detect and attack malicious web traffic, including web app attacks listed on the OWASP Top 10.

Network Zones

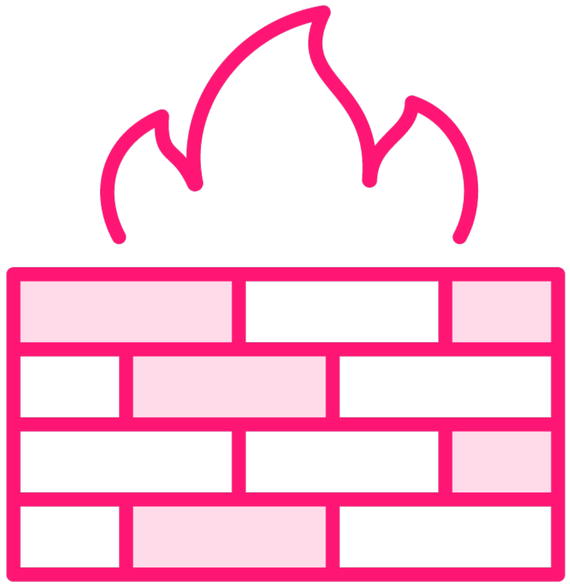


Chris Jackson

Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

Zones of Trust



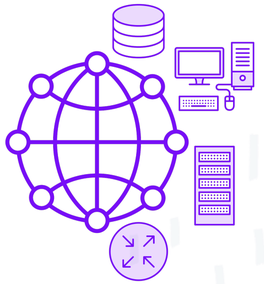
Untrusted



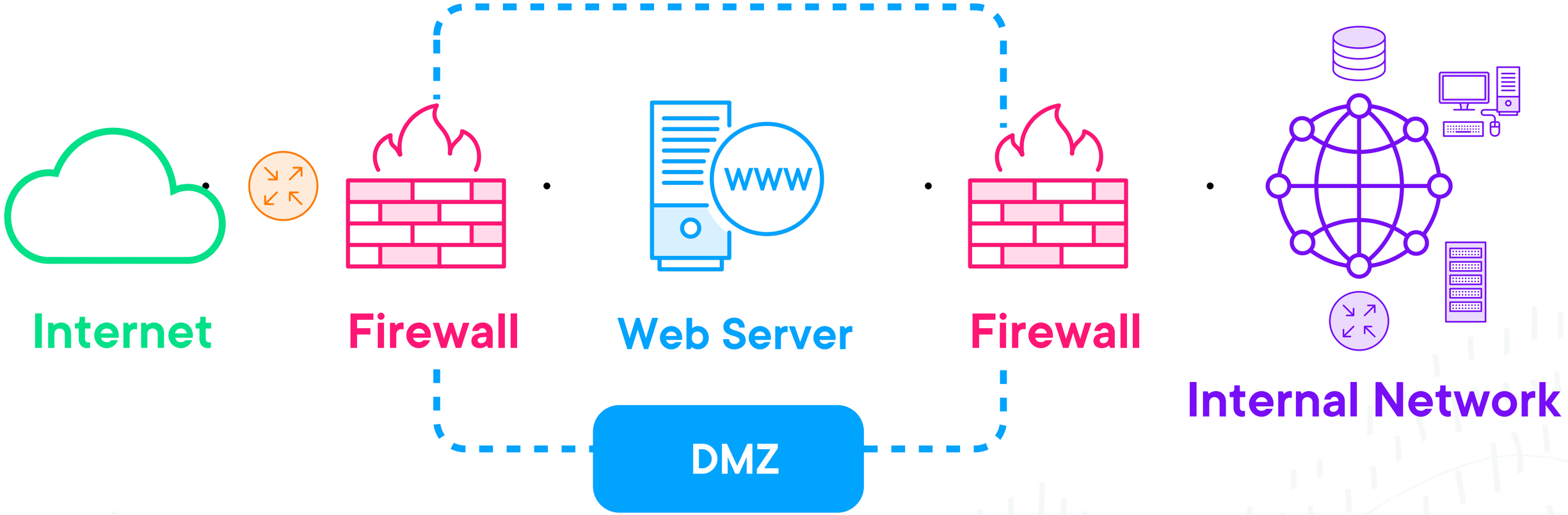
Semi-Trusted



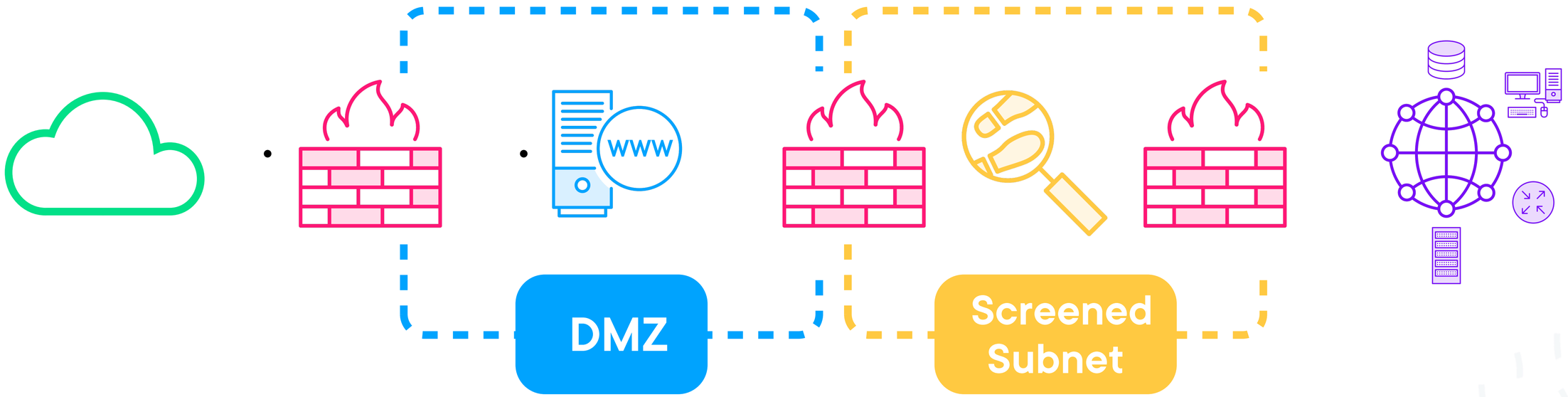
Trusted



Demilitarized Zone (DMZ)



3 Tier Firewall Architecture



Zero Trust Network Architecture (ZNTA)



Chris Jackson

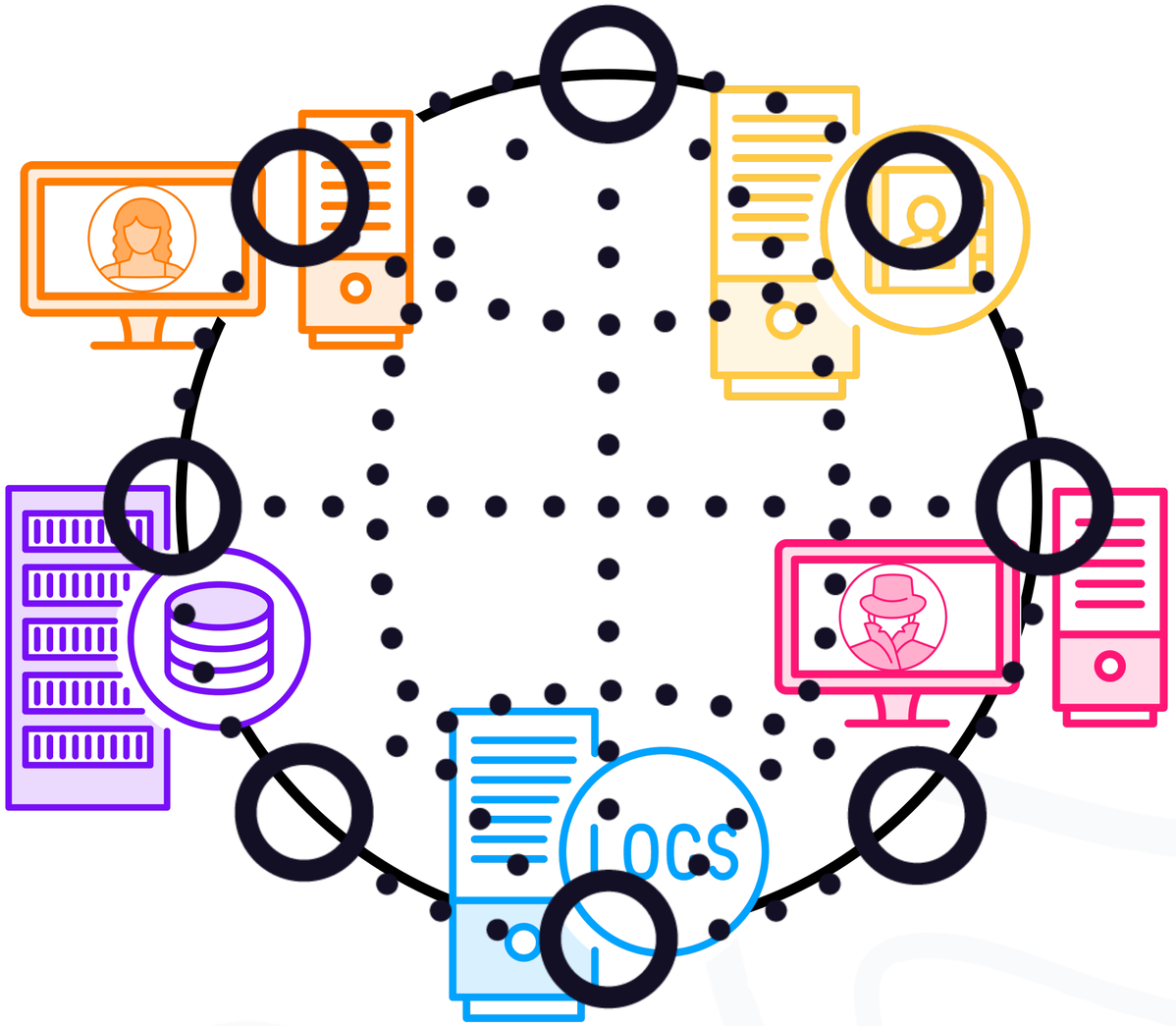
Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

Zero Trust

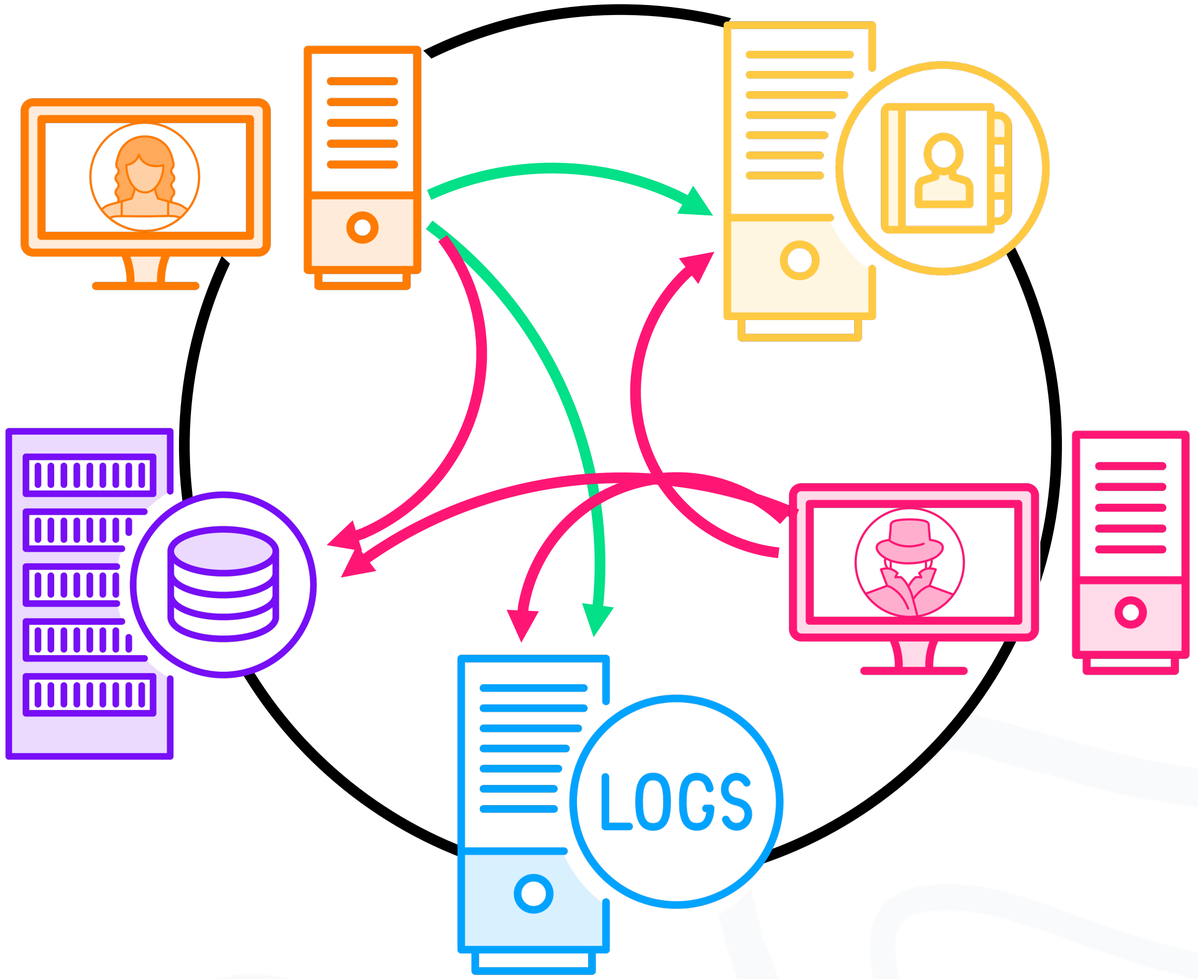
Never Trust, Always Verify

A security architecture model that eliminates implicit trust by requiring strict identity verification and continuous authentication for every user, device, and application before granting access to any resource, regardless of their location or network connection.

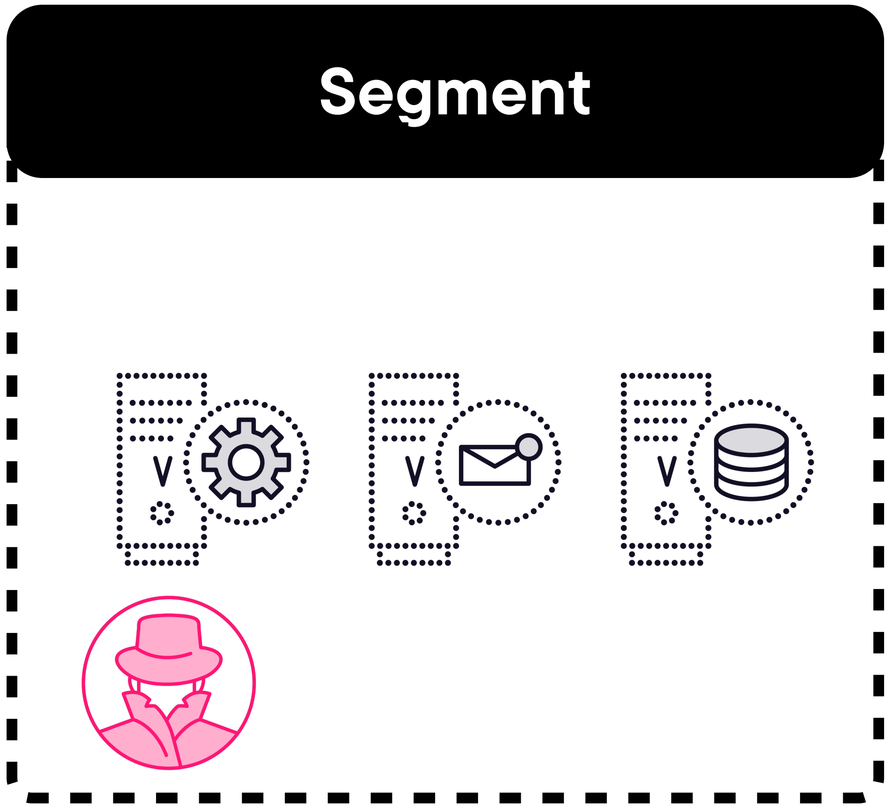


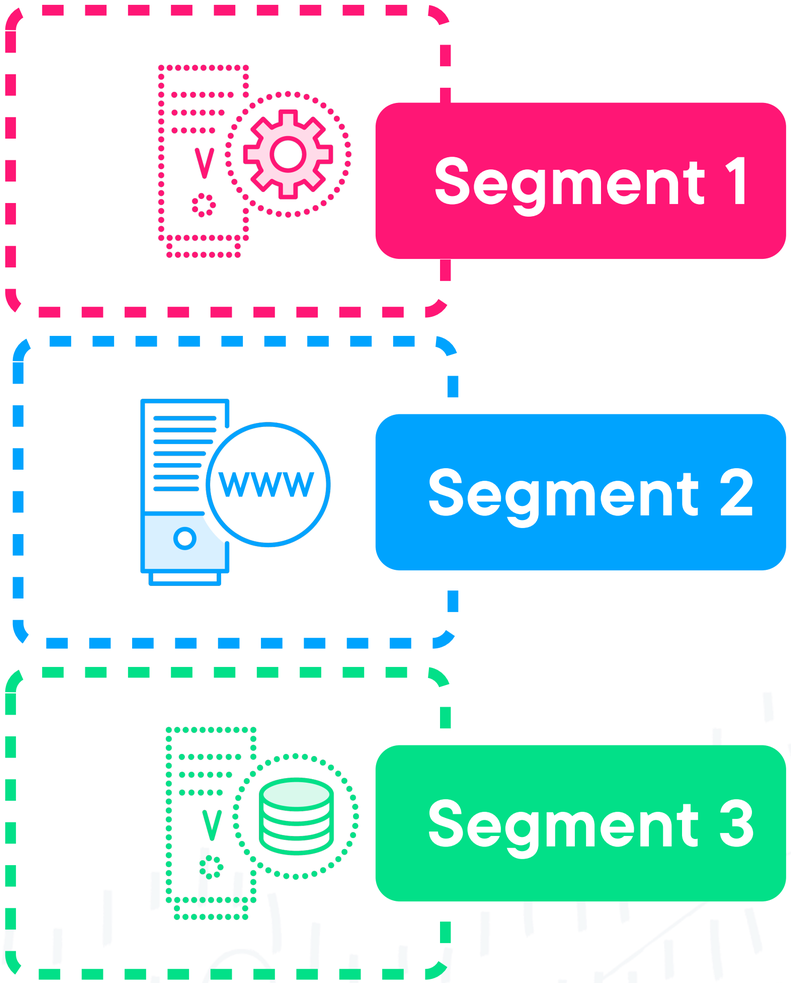
Zero Trust

- Authentication
- Least Privilege
- Assume Breach

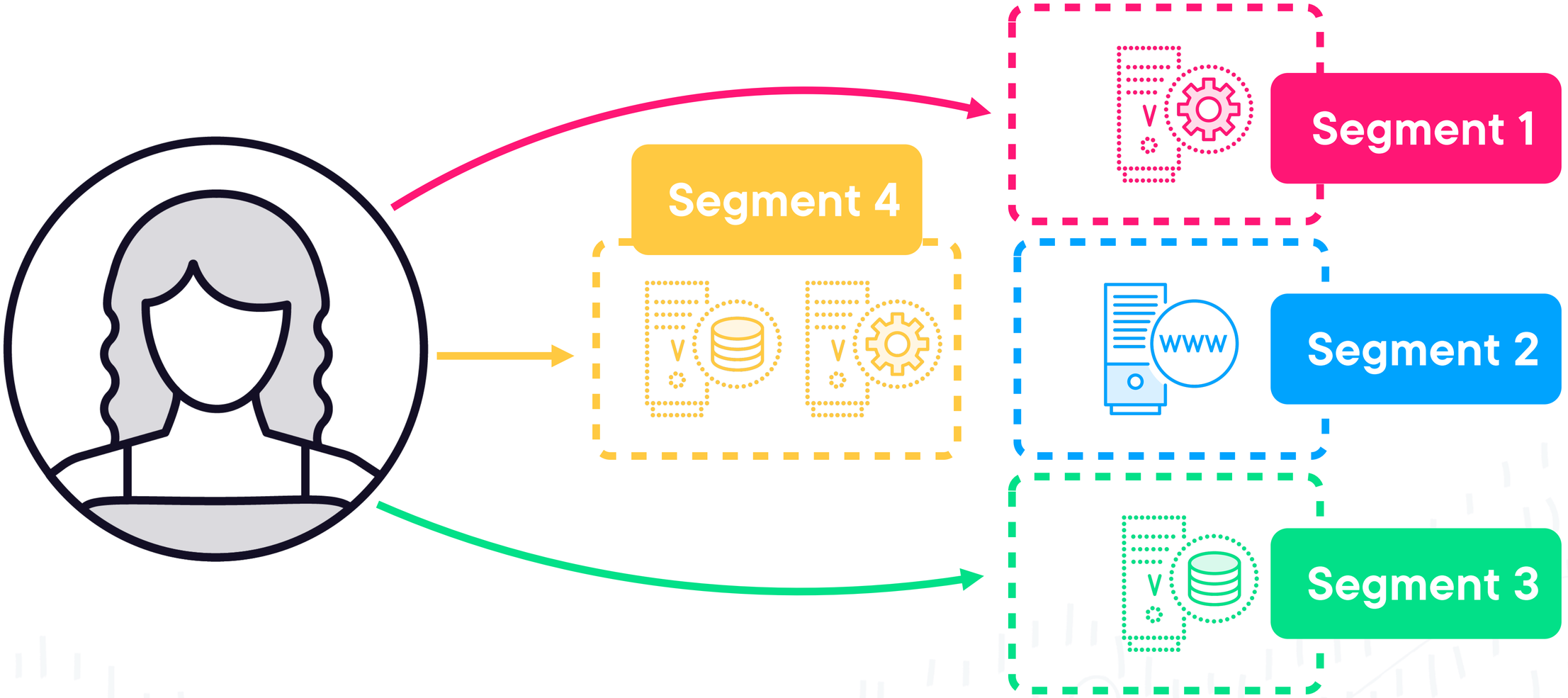


Network-based Microsegmentation

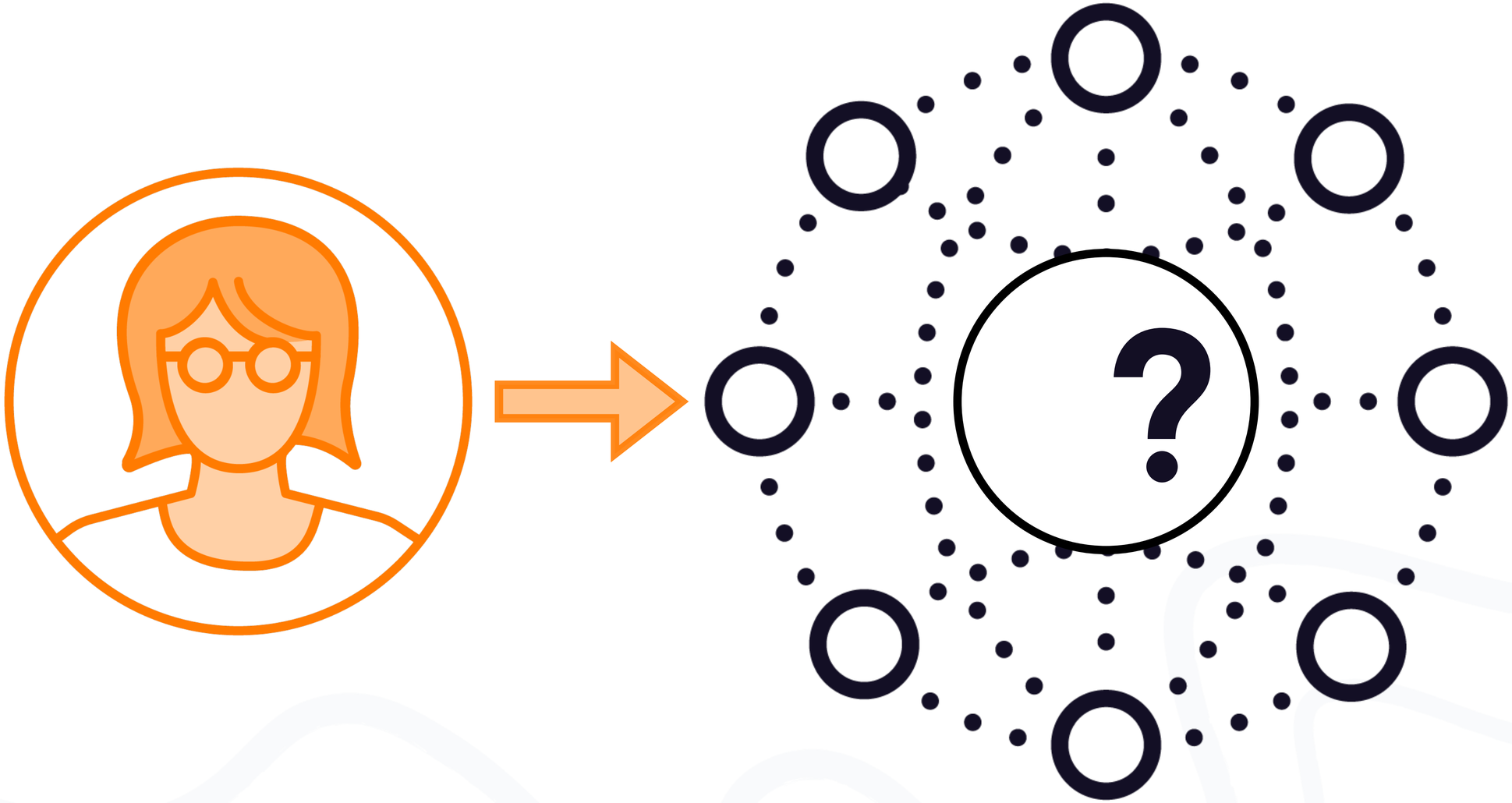




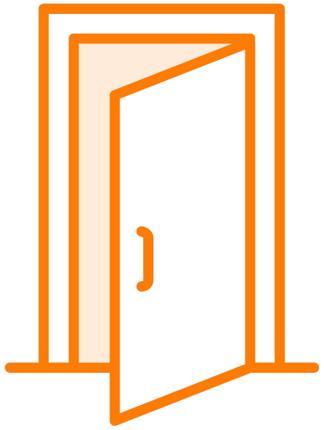
Identity-based Microsegmentation



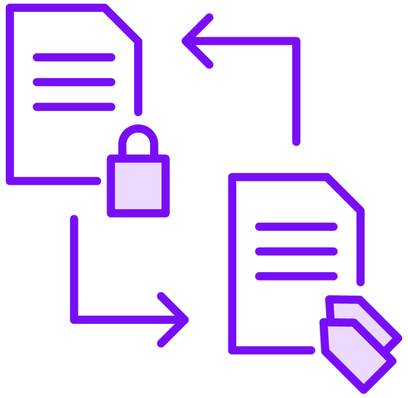
Software Defined Perimeter (SDP)



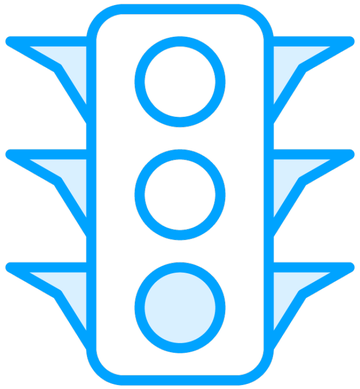
Zero Trust Components



Client

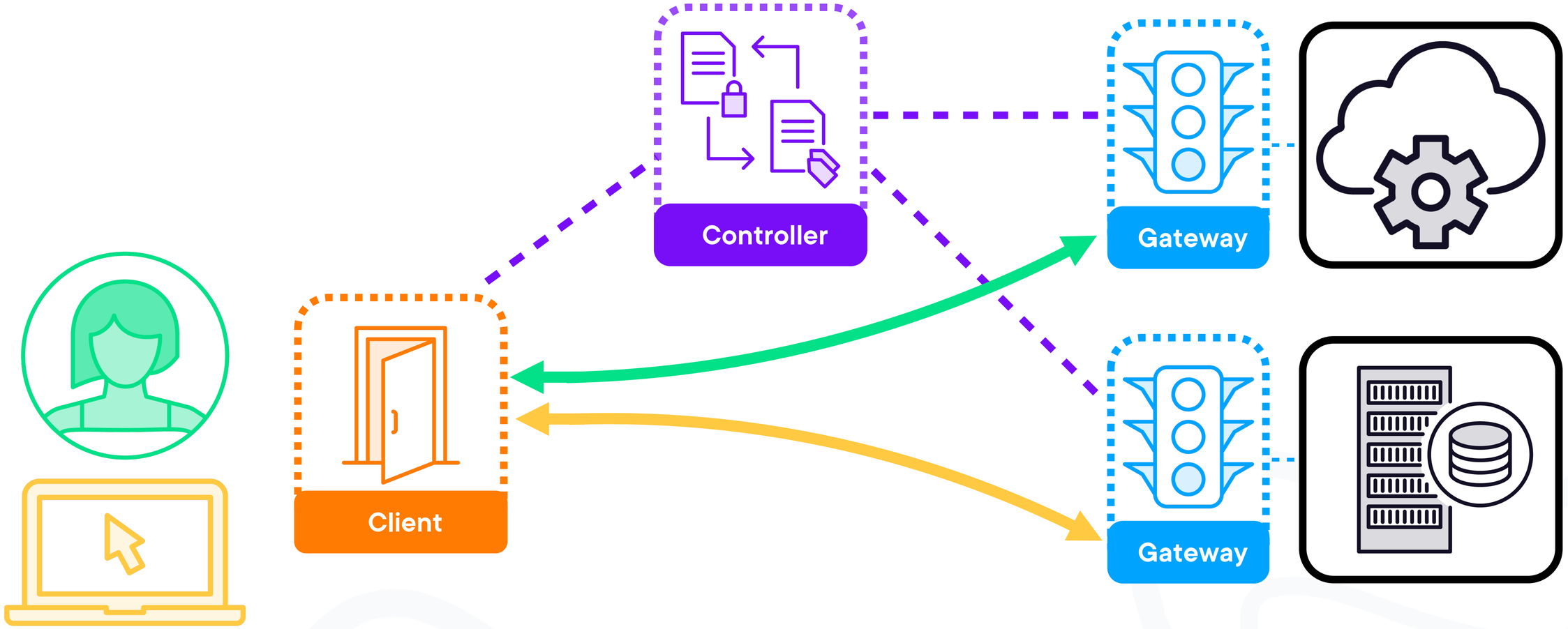


Controller



Gateway

Software Defined Perimeter (SDP)



Routing Protocol Security

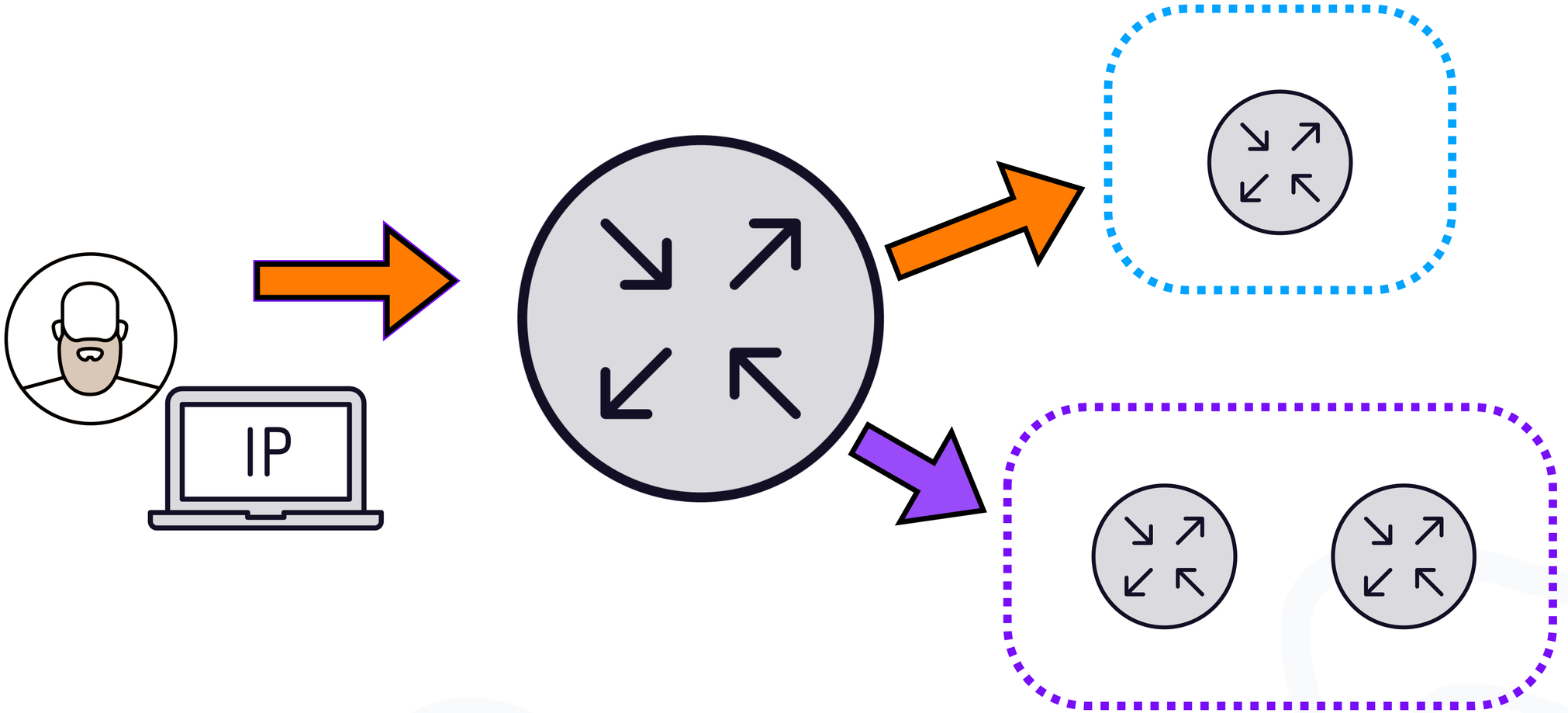


Chris Jackson

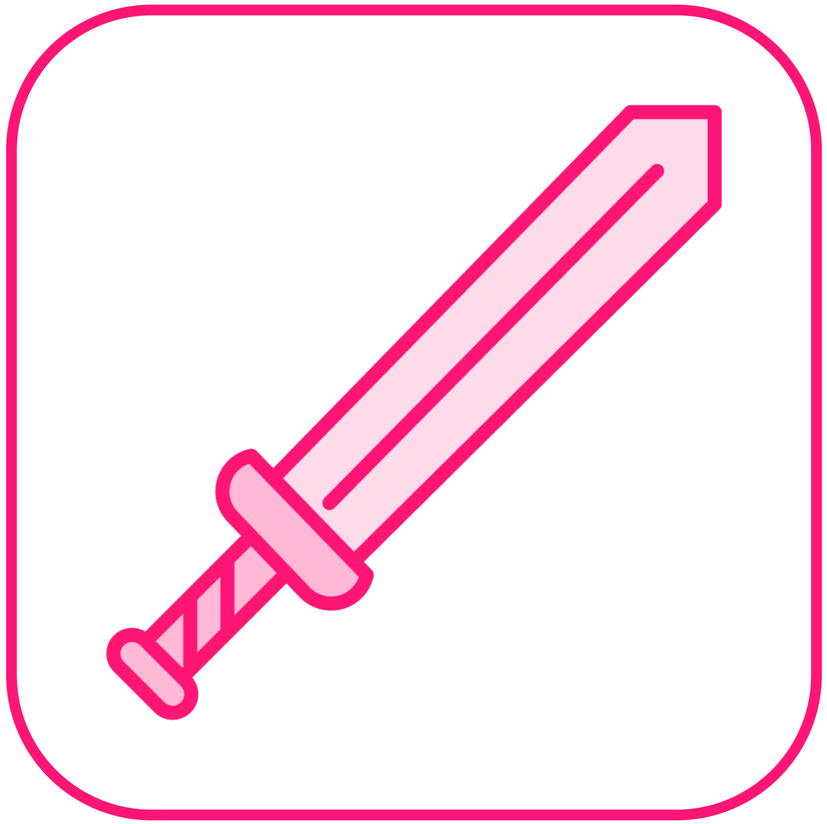
Pluralsight Author

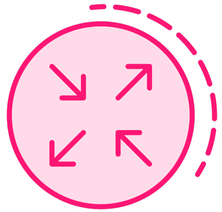
ChrisJacksonMSIT | CyberTitanLLC.com

IP Source Routing



OSPF Security





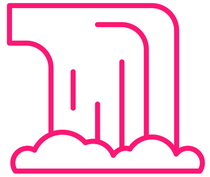
Remote False Adjacency



Spoofing

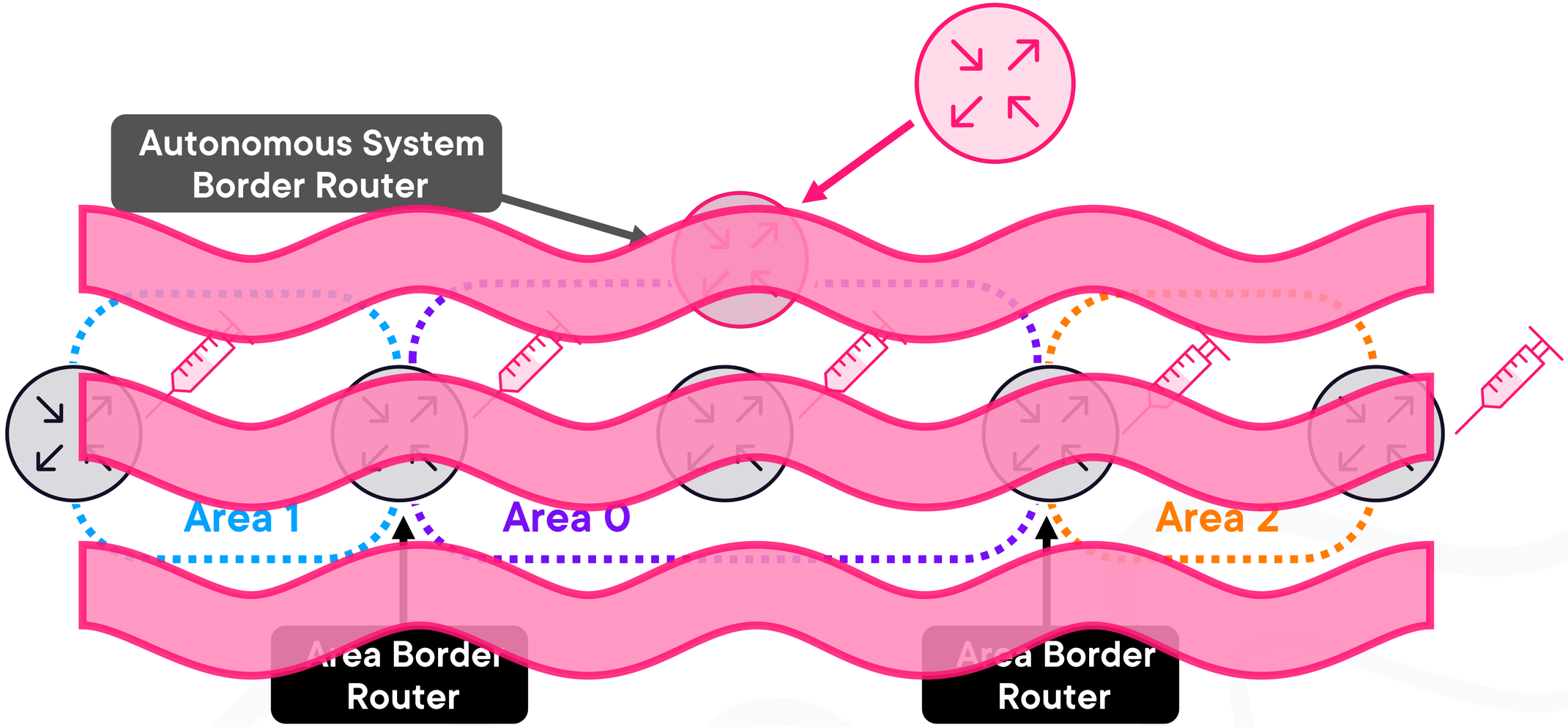


Route Injection

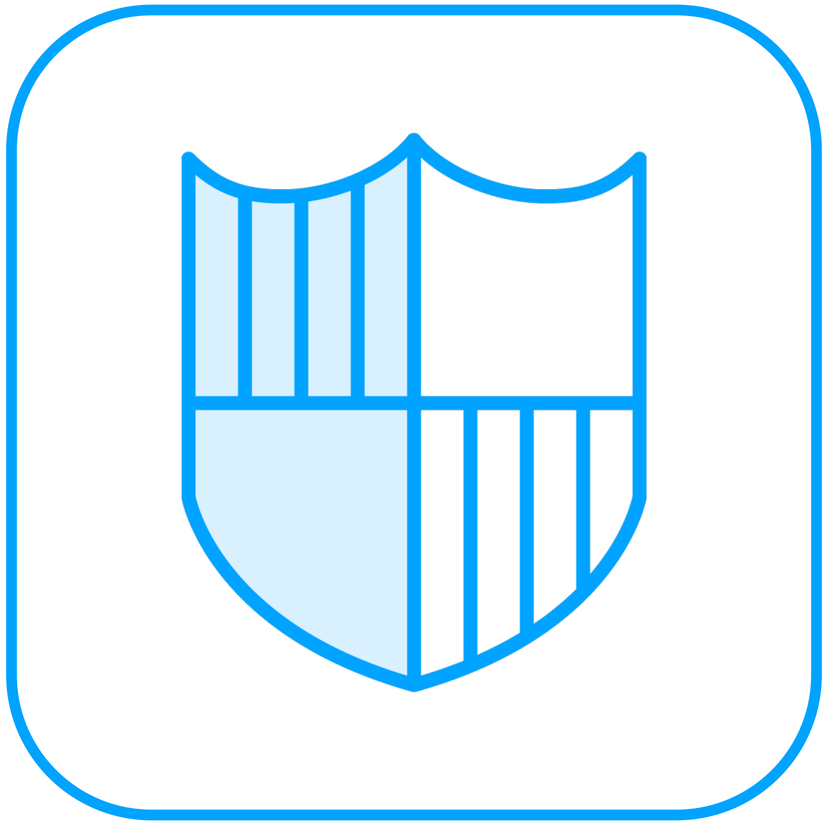


Flooding

OSPF Security

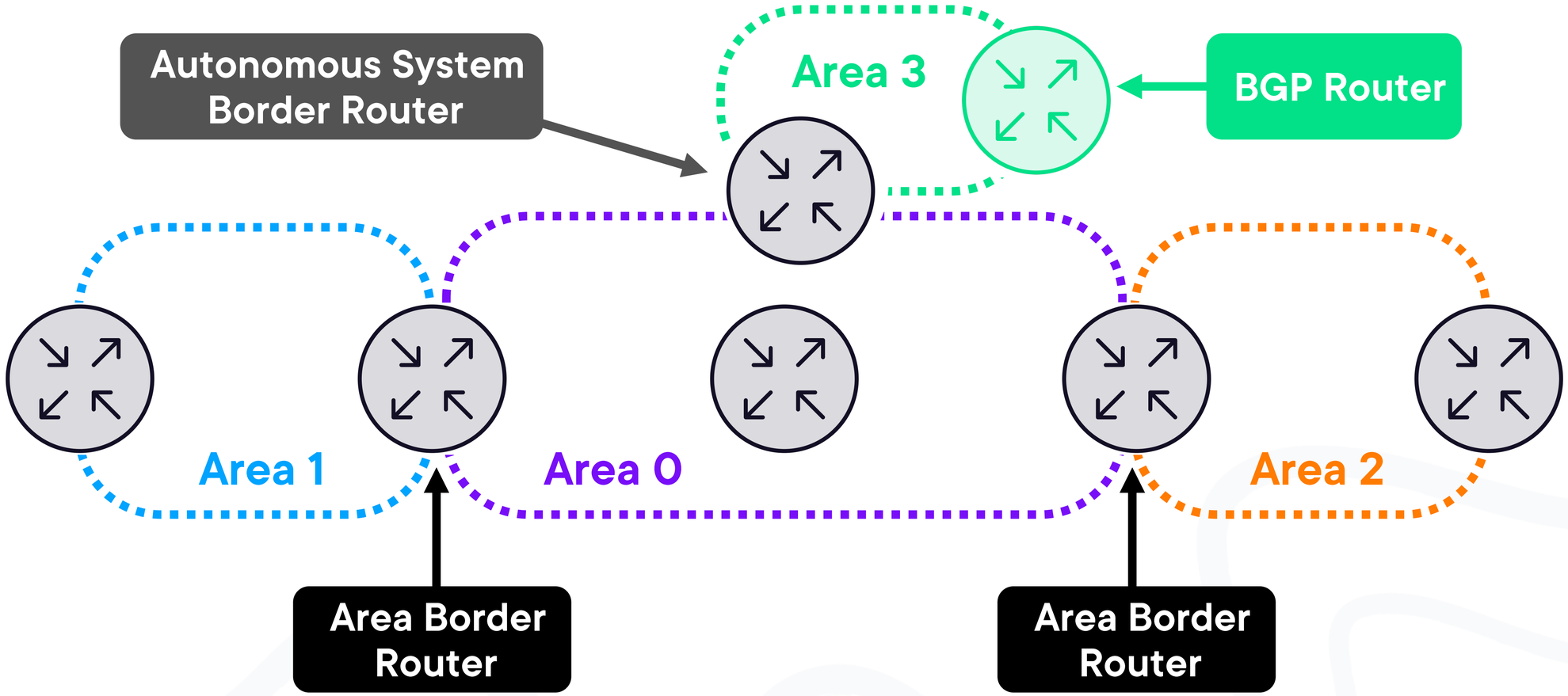


OSPF Security

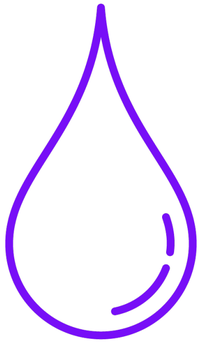


- Authentication
- Area Segmentation
- Time-To-Live
- Logging and Monitoring

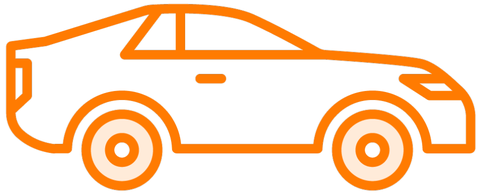
OSPF Security



BGP Security Risks



Route Leak

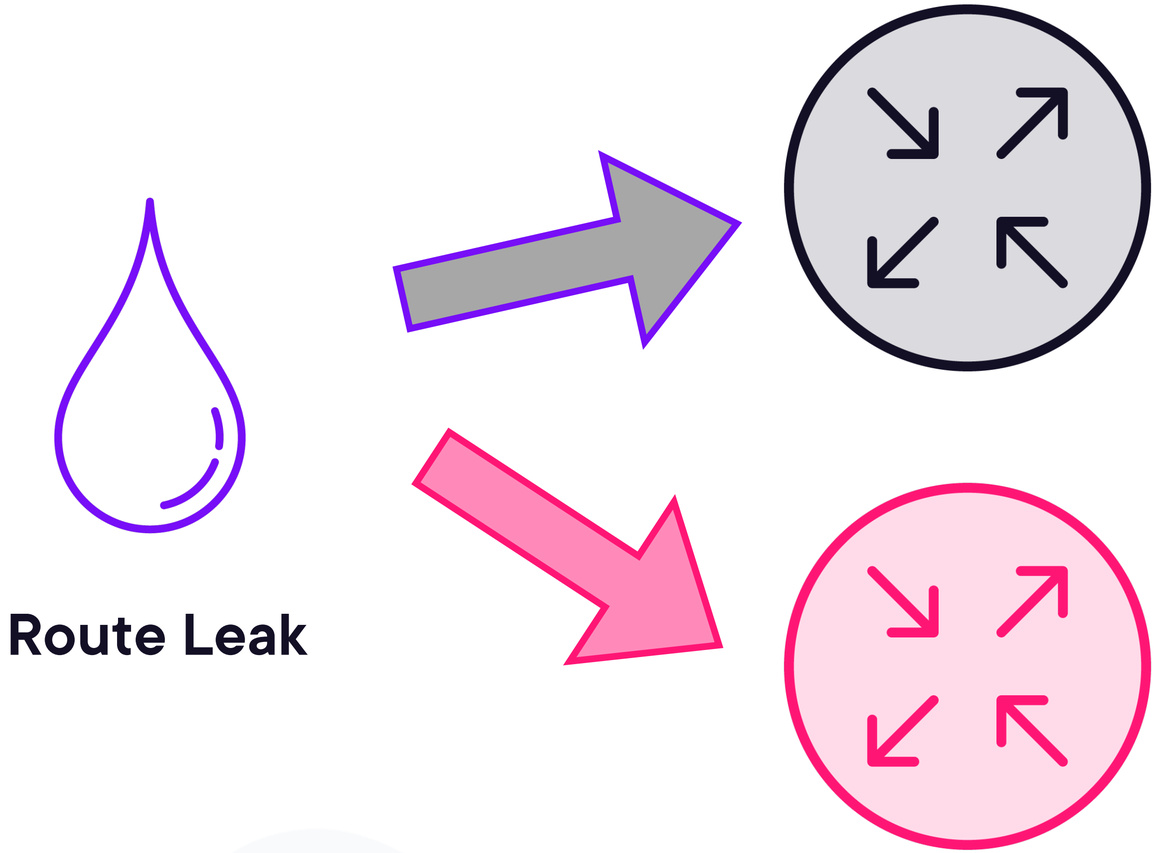


Hijacking

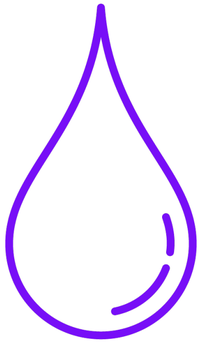


Flooding

BGP Security Risks

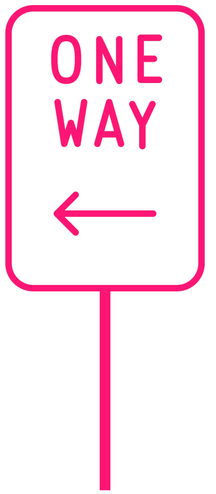


BGP Security Risks



Route Leak





BGP Security Controls



AuthN



Filtering



Route Origin



TTL

AAA and Remote Access



Chris Jackson

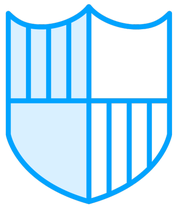
Pluralsight Author

ChrisJacksonMSIT | CyberTitanLLC.com

AuthN, AuthZ, and Accounting



Authentication

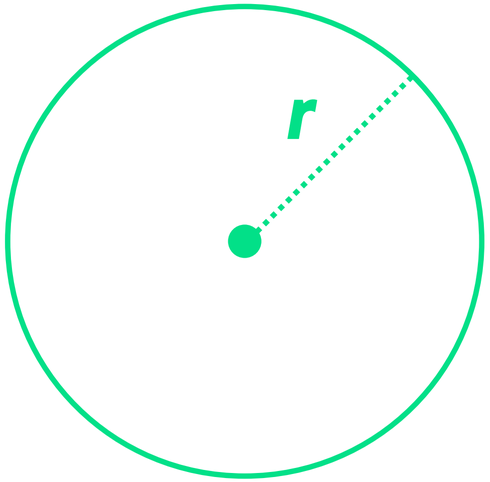


Authorization



Accounting

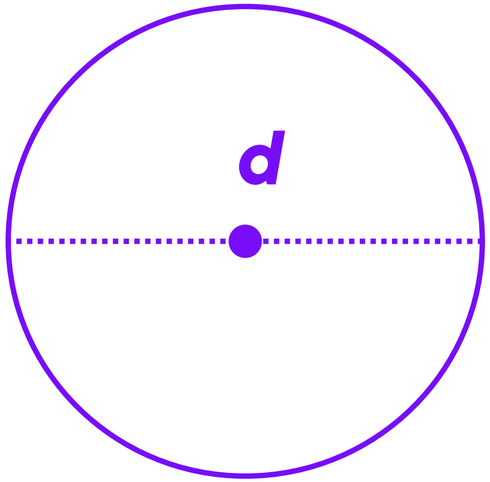
AAA Protocols



RADIUS

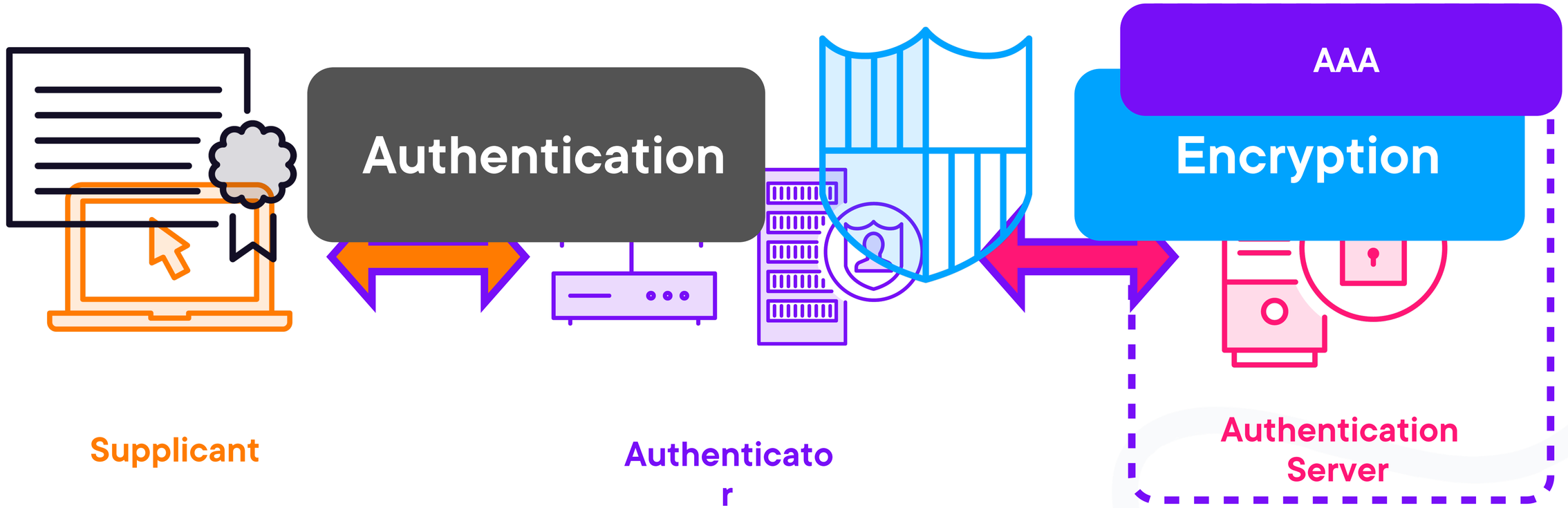


TACACS+

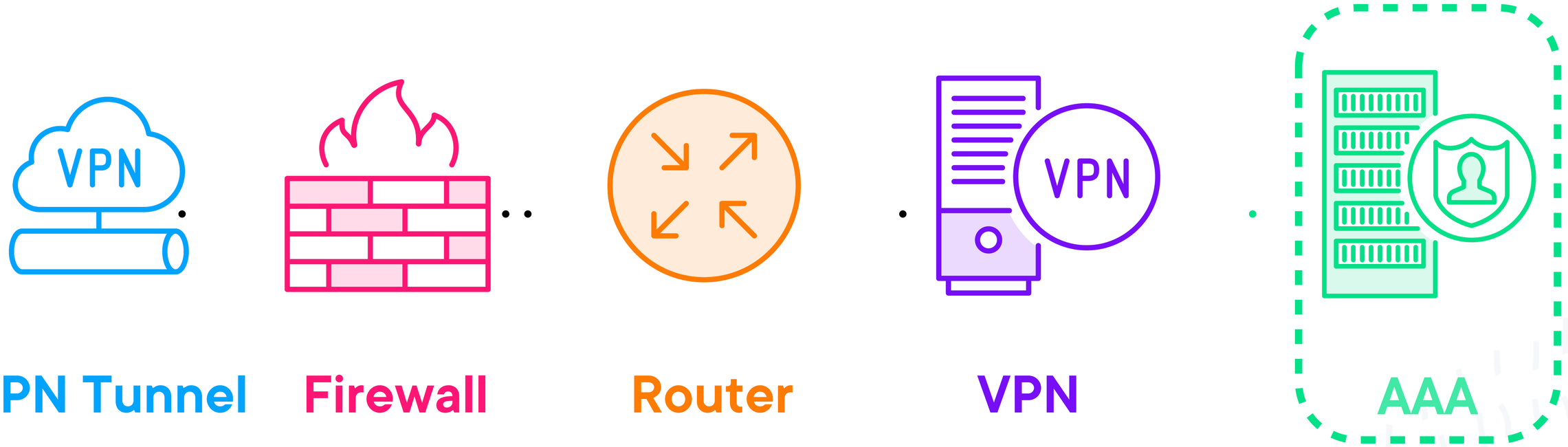


Diameter

Wireless Connection Security



VPN Architecture

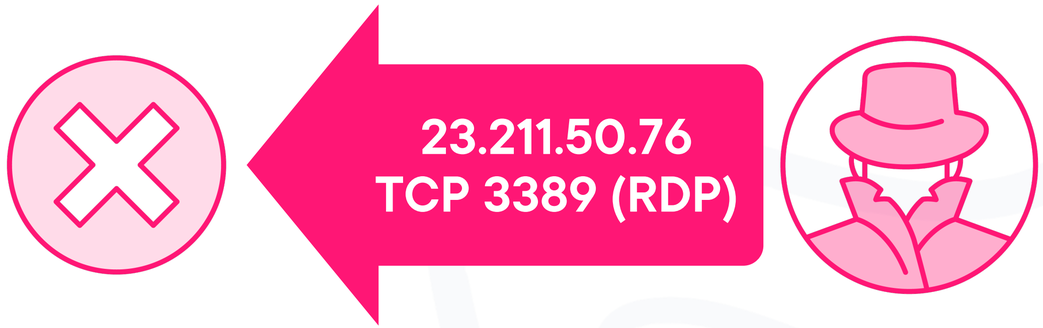


Access Control Lists (ACLs)

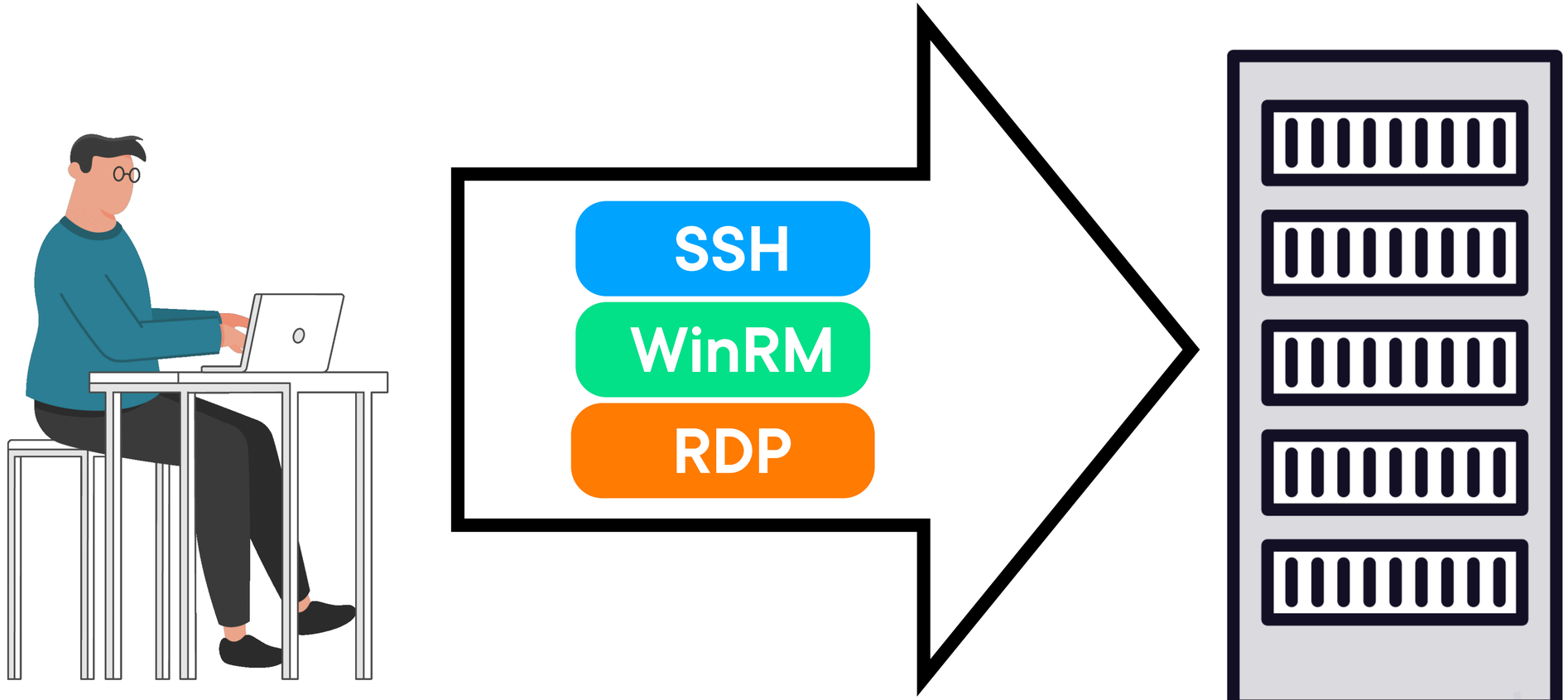




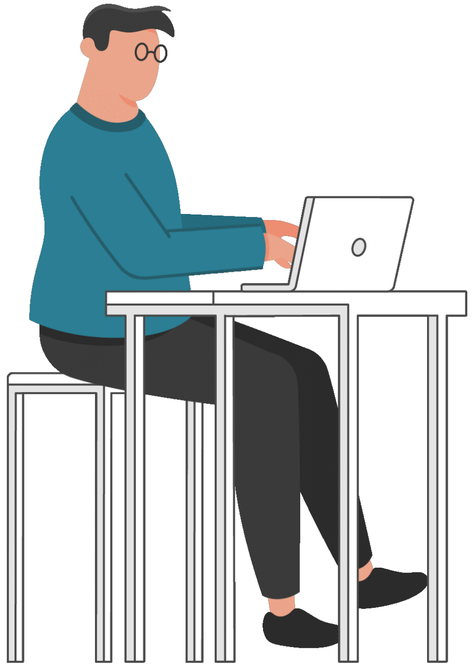




Remote Management

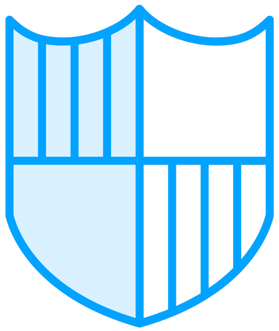


Remote Management





Authenticatio
n



Encryption

