

Playing with DNS Poisoning Attacks



Dale Meredith

MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | [Twitter: @dalemeredith](https://twitter.com/dalemeredith) | [Linkedin: dalemeredith](https://www.linkedin.com/in/dalemeredith)

“I’ve been imitated so well I’ve heard people copy my mistakes.”

Jimi Hendrix



Human's capacity to remember a name is greater than our ability to remember a long set of numbers

DNS is the protocol that translates a domain name into an IP address

www.pluralsight.com => 52.26.113.205

Review DNS Roles

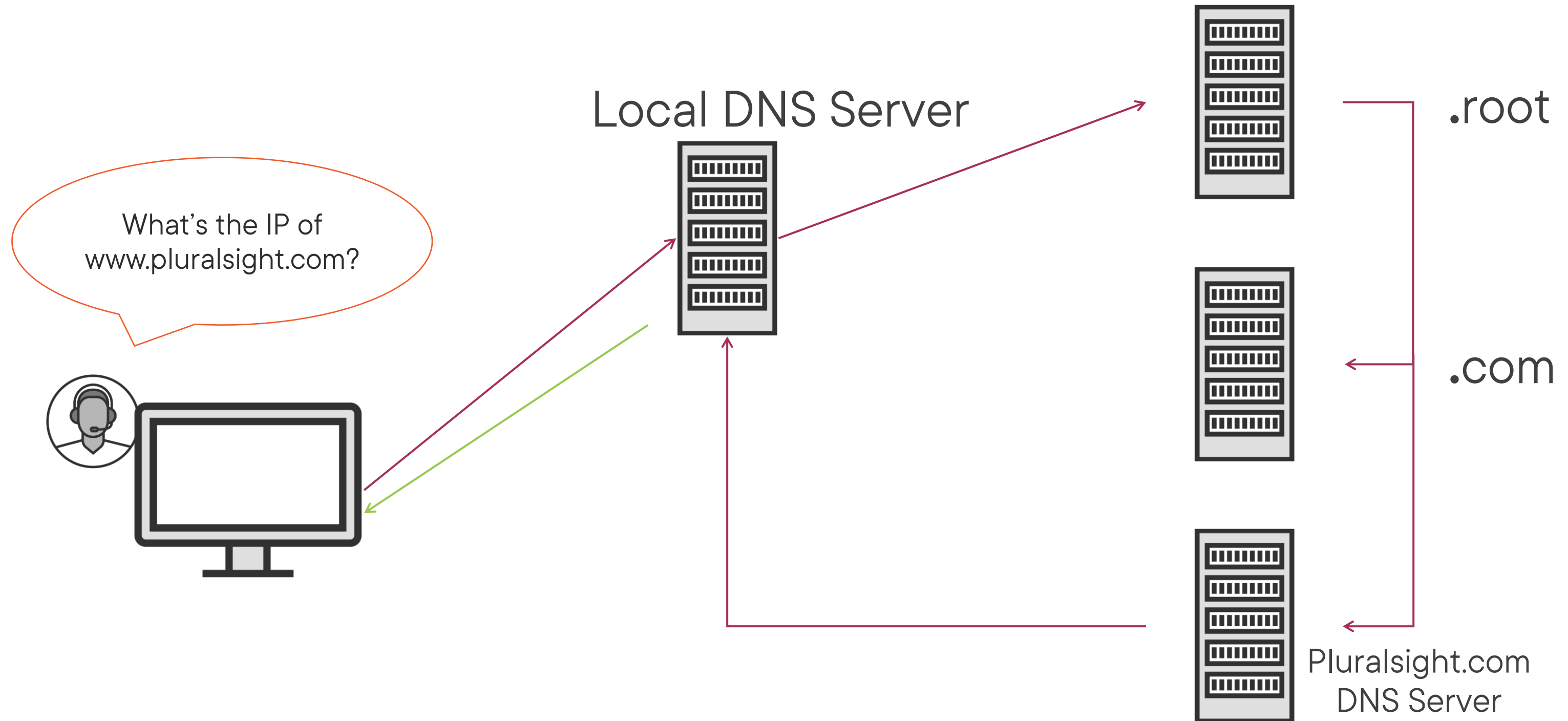


Tables

- Internal
- External

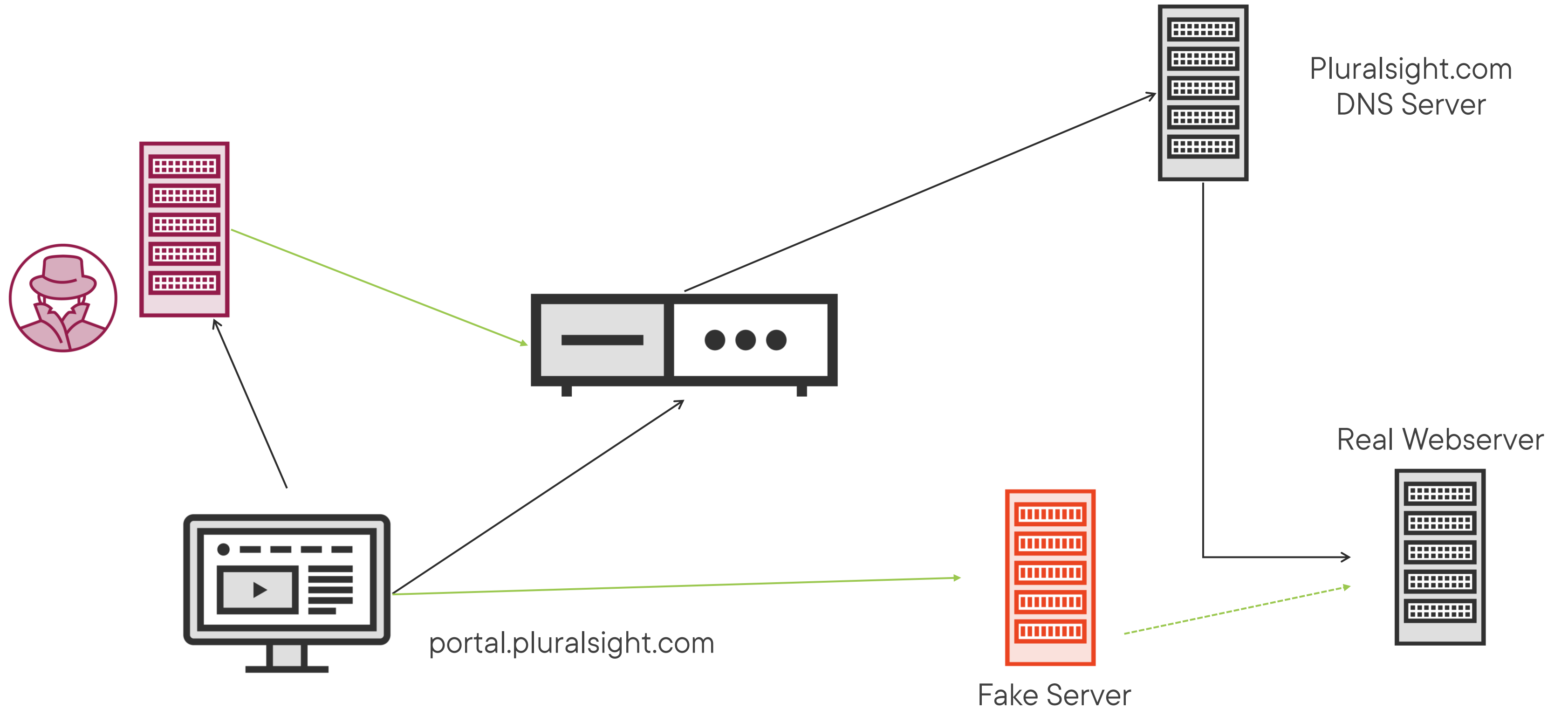
Authoritative vs Non-authoritative

Under the Hood

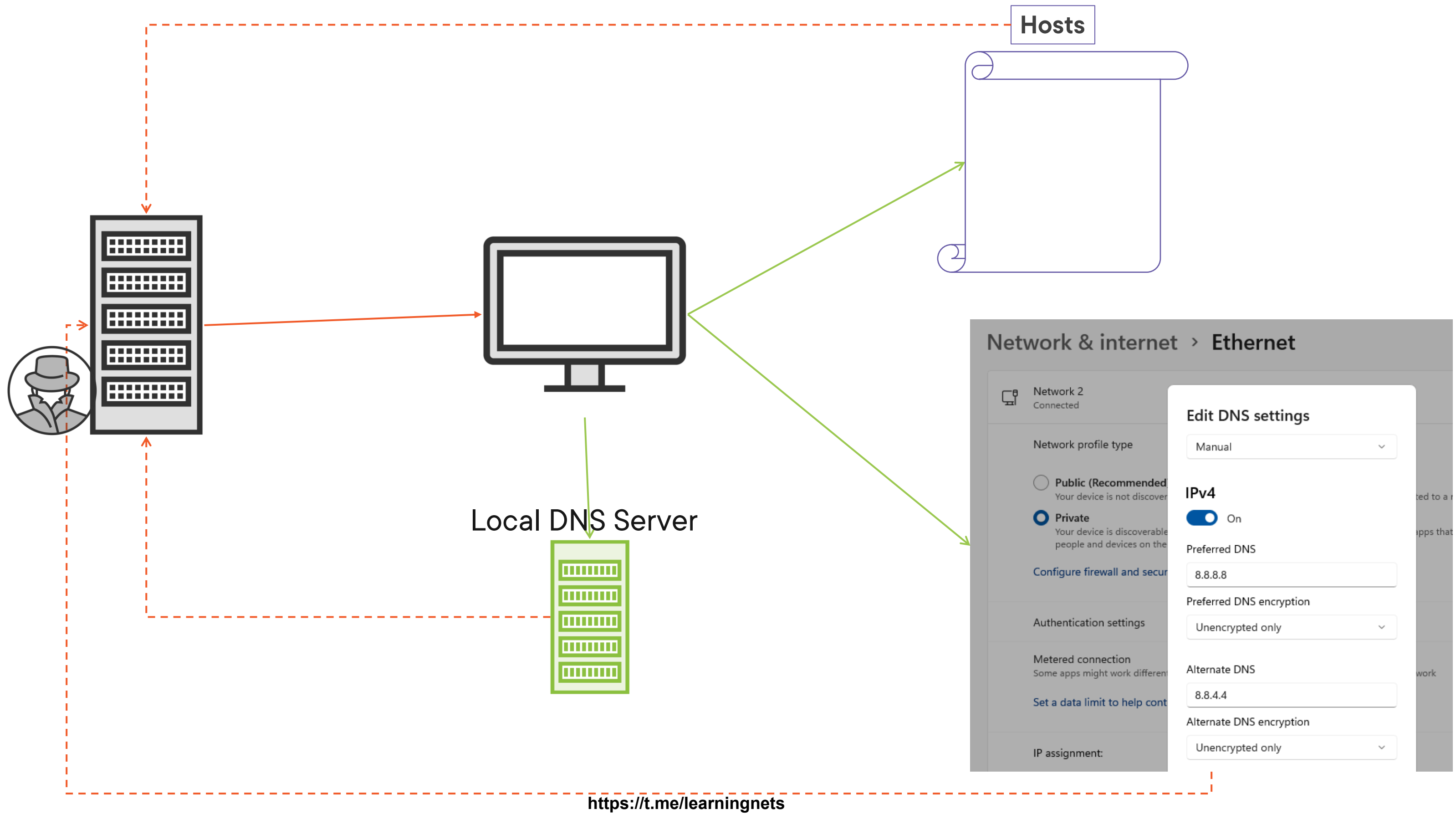


Intranet DNS Spoofing

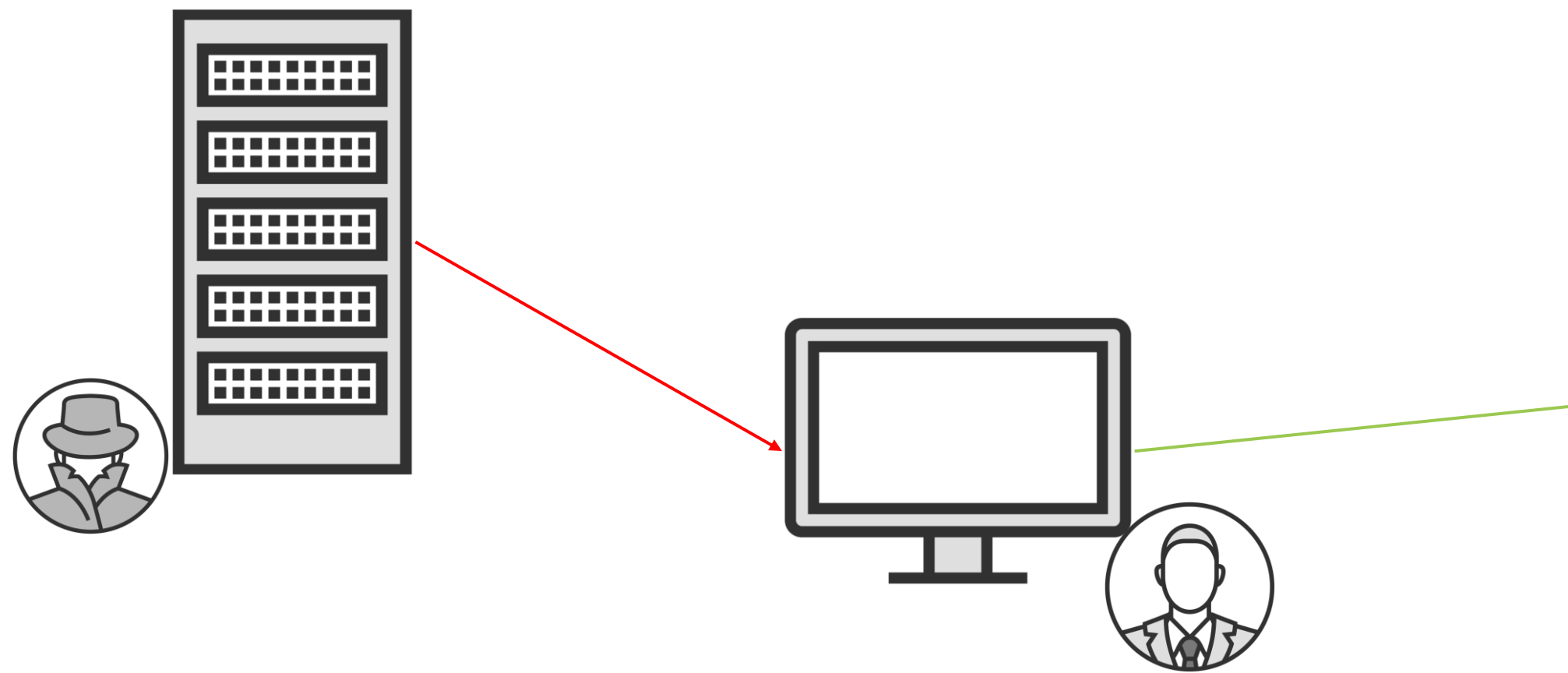
Under the Hood



Internet DNS Spoofing



Proxy Server DNS Poisoning



Network & internet > Proxy

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatic proxy setup

Automatically detect settings

Use setup script
Off

Manual proxy setup

Use a proxy server
On

Edit proxy server

Use a proxy server
 On

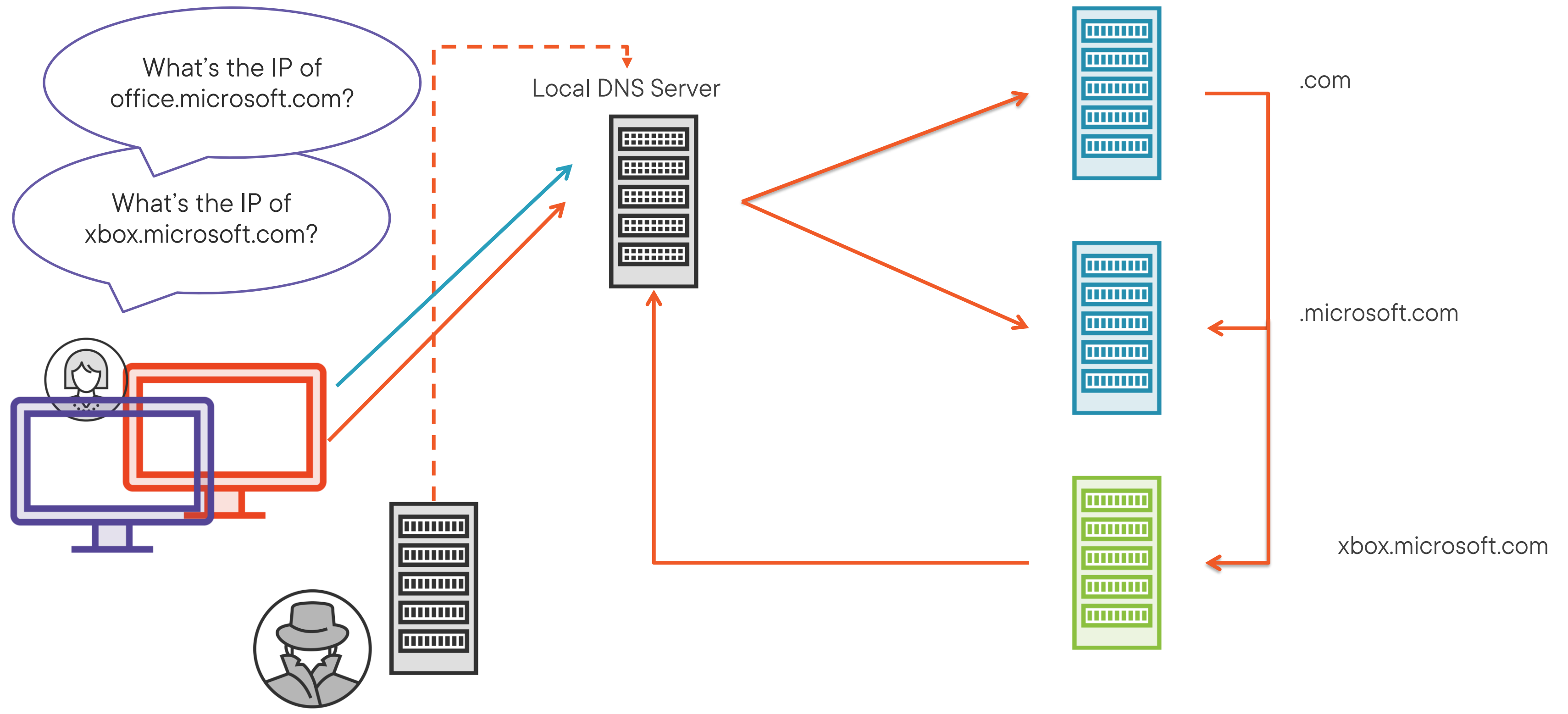
Proxy IP address Port

Use the proxy server except for addresses that start with the following entries.
Use semicolons (;) to separate entries.

Don't use the proxy server for local (intranet) addresses

Save Cancel

DNS Cache Poisoning



DNS Poisoning Tools



DNS Spoof



DNS-poison



Ettercap



Evilgrade



Tornado



A

Demo



Poison DNS

DNS Spoofing Countermeasures

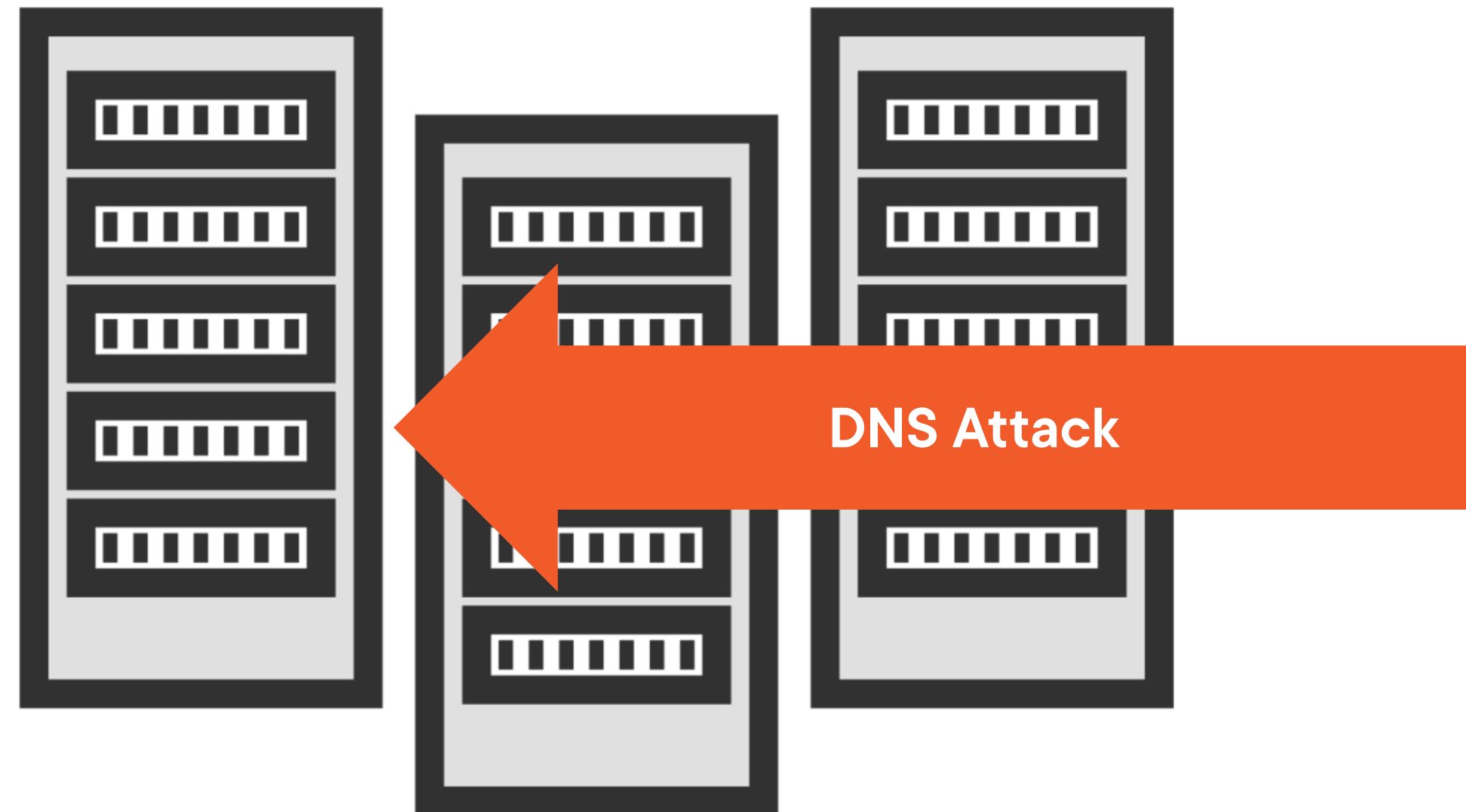
Countermeasures



Defending a Network against a DNS Spoofing Attack

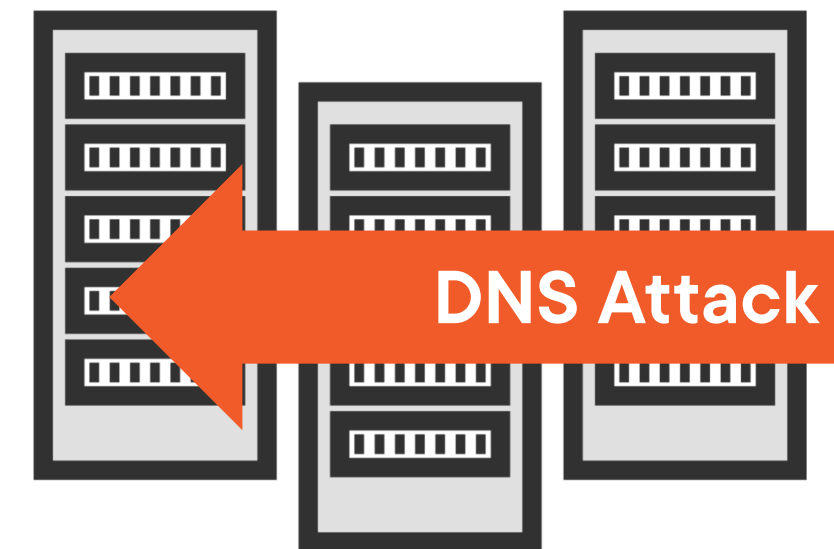
Countermeasures

- DNSSEC
- Use a Secure Socket Layer (SSL)
- Resolve all queries to a local DNS server
- Block requests sent to external servers
- Restrict external DNS lookup with a firewall
- Implement an (IDS)
- Configure DNS to use a new random source port



Countermeasures

A plethora
of choices



And more..

Learning Check

Learning Check



Intranet spoofing



Hosts



Internet spoofing



DNSSEC



Random port source



Up Next:

Implementing Countermeasures
