學術網路DDoS攻防實務

Reliable Security Always™

威脅服務可用性：DDoS攻擊

DDoS攻擊不只一種

VOLUMETRIC

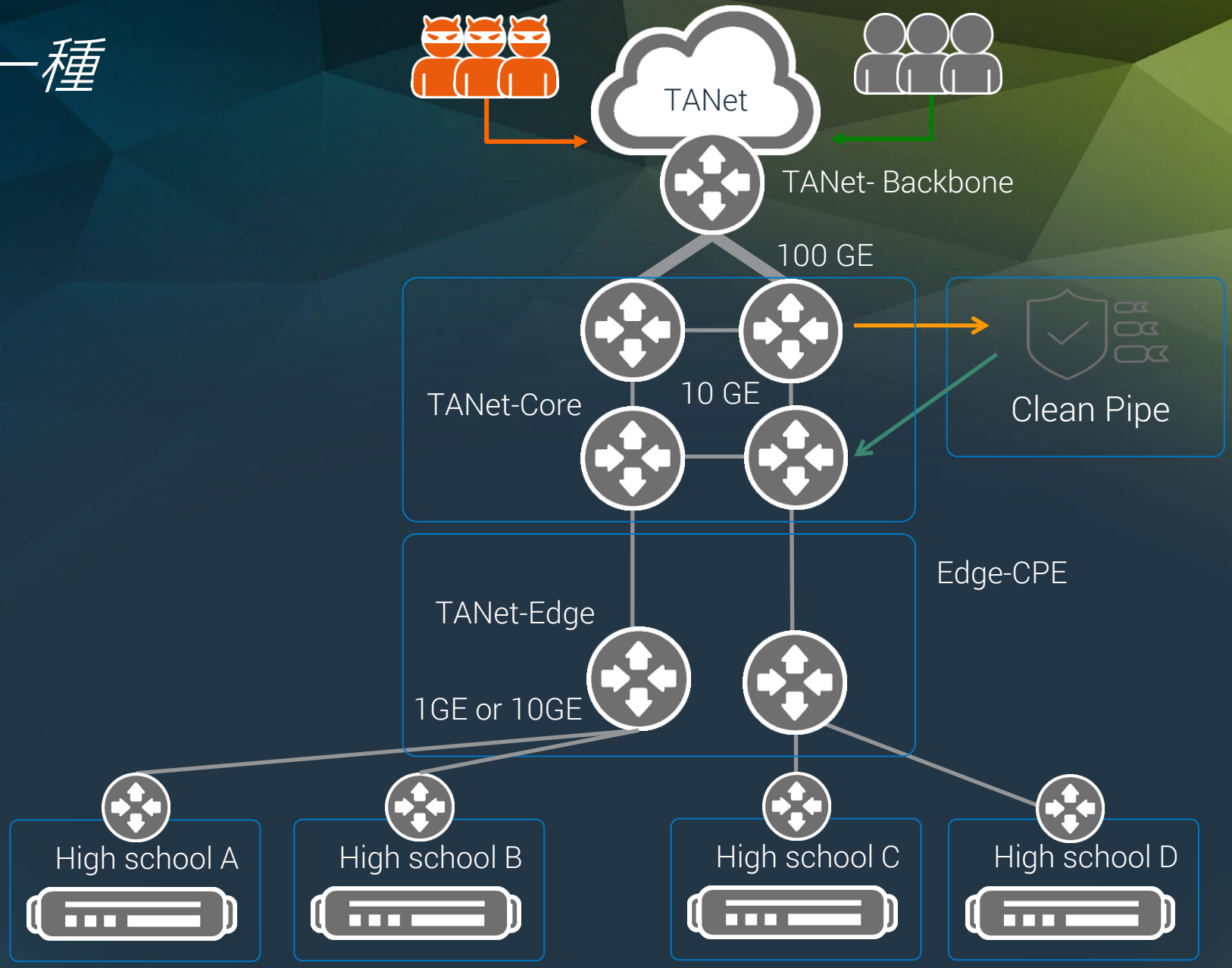
- DNS amplification
- NTP amplification
- SSDP amplification
- UDP Flood

NETWORK LAYER

- Fragmentation
- SYN floods
- Ping floods
- Etc.

APPLICATION LAYER

- Slowloris
- HTTP GET floods
- R.U.D.Y.
- Etc.



IoT時代來臨,DDoS變得更簡單

美國大學遭到DDoS攻擊，「凶手」竟然是校內的自動販賣機、路燈

美國電信商Verizon揭露一所美國大學遭到DDoS攻擊，在追查下竟發現來自校內為數約5000台的物連網裝置，包含連網路燈、自動販賣機等，所幸駭客操控手法不夠高明，校方最後取回這些連網裝置的控制權。

讚 4.6 萬 按讚加入iThome粉絲團 讚 0 分享

文/ 陳文義 | 2017-02-14 發表

Verizon在即將發表的2017年資料安全報告的預覽文章中揭露了這起因物聯網(IoT)裝置導致的DDoS攻擊事件。這間未被公開名稱的大學，起初是發現校園網路速度明顯變慢，進而追蹤到DNS伺服器有大量詭異的域名查詢，有許多包括海鮮名稱的子網域查詢需求，顯然是透過殭屍網路傳送至該校DNS伺服器，進一步調查後發現，這些查詢需求都發自該校區內的IoT裝置。

攻擊來自於校內！？

Mirai殭屍網路的威脅


iThome

Dyn遭大規模DDoS攻擊，Mirai殭屍網路脫不了關係

Dyn與資安公司合作調查上周五遭大規模DDoS攻擊事件，指出駭客先後共發動三波攻擊，是一次非常精密的攻擊行動，涉及上千萬個IP位址，在資安公司協作下發現部份的攻擊來自Mirai殭屍網路。

文/ 陳曉莉 | 2016-10-25 發表

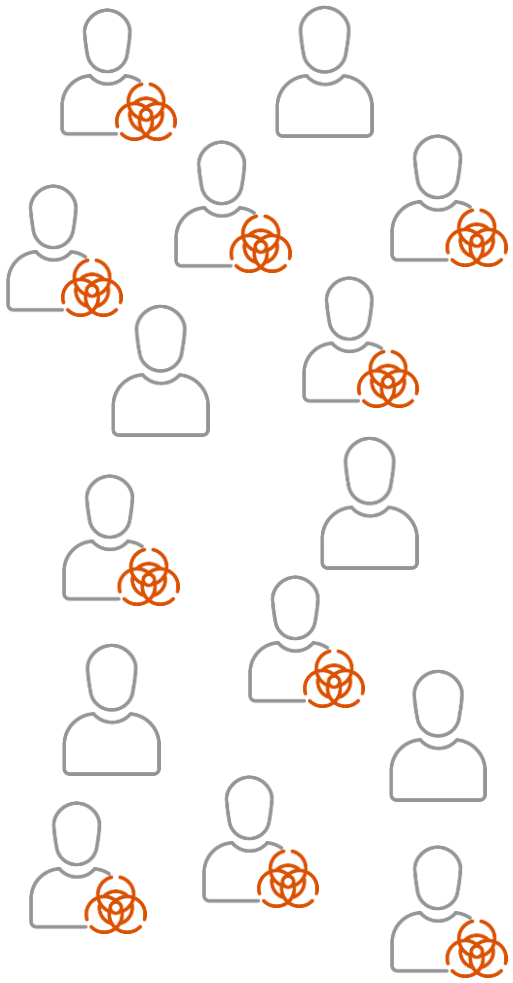
讚 5 萬 按讚加入iThome粉絲團 讚 0 分享 G+

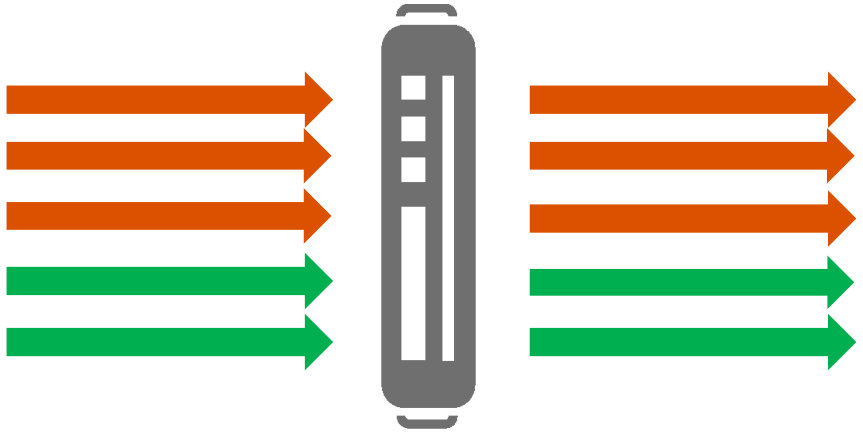
Dyn PRODUCTS RESOURCES SUPPORT COMPANY Search Dyn SIGN IN

Dyn Statement on 10/21/2016 DDoS Attack

美國域名系統提供商Dyn公司的DNS服務系統在2016-10-21遭到大規模的DDoS攻擊，影響了包括Twitter、Amazon、Spotify及Netflix等使用該公司服務的網路公司，這個攻擊據信大部分是由感染Mirai惡意軟體的物聯網裝置(包括印表機、網路監控攝影機和家庭路由器等)組成的殭屍網路所發動，尖峰流量估計達到1.2Tbps，是迄今為止規模最大的網路攻擊。

目前防禦方式？





NGFW or IPS

Web Service

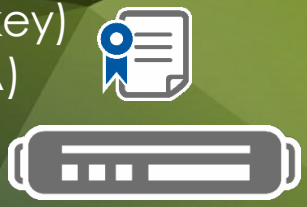
DNS Service

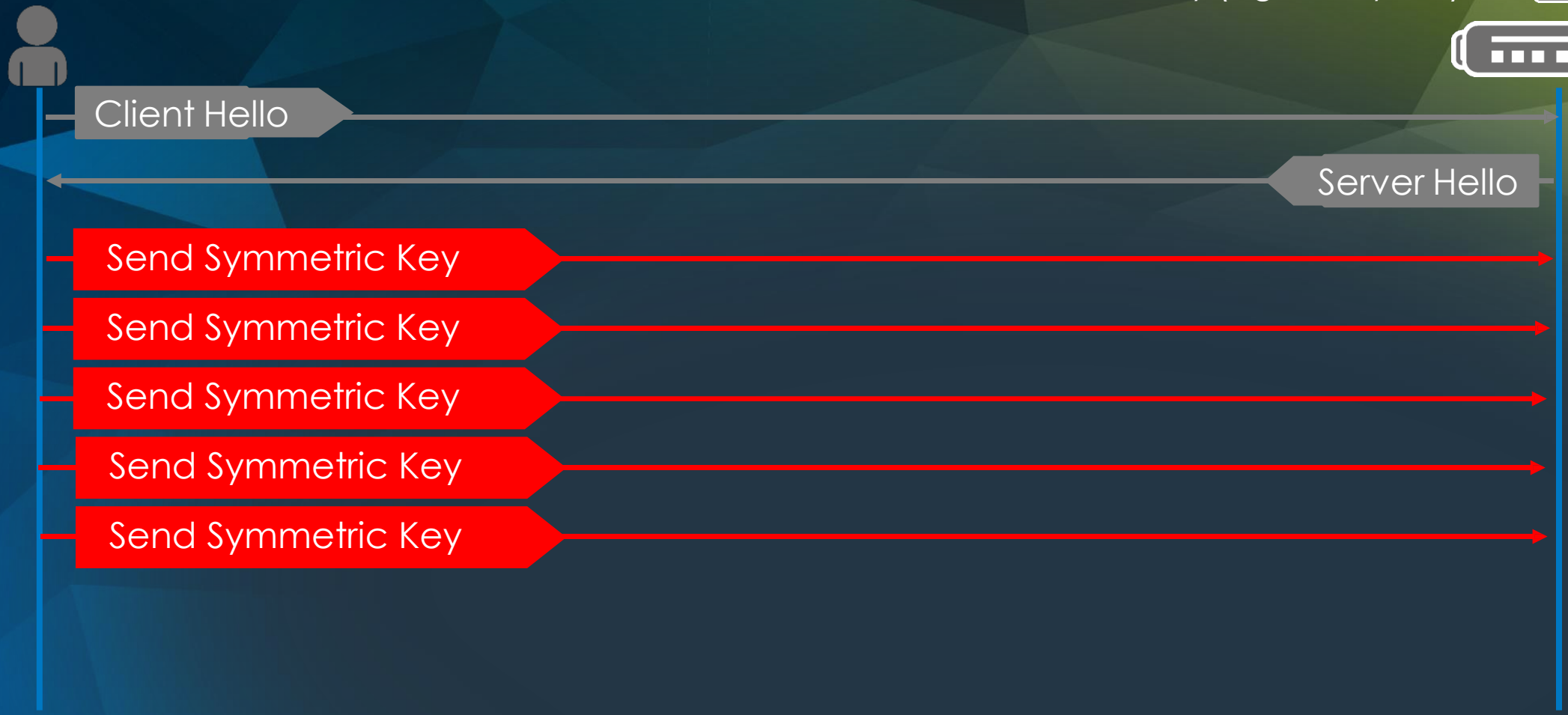
真能防禦DDoS攻擊？

小流量但能癱瘓伺服器的應用層攻擊手法

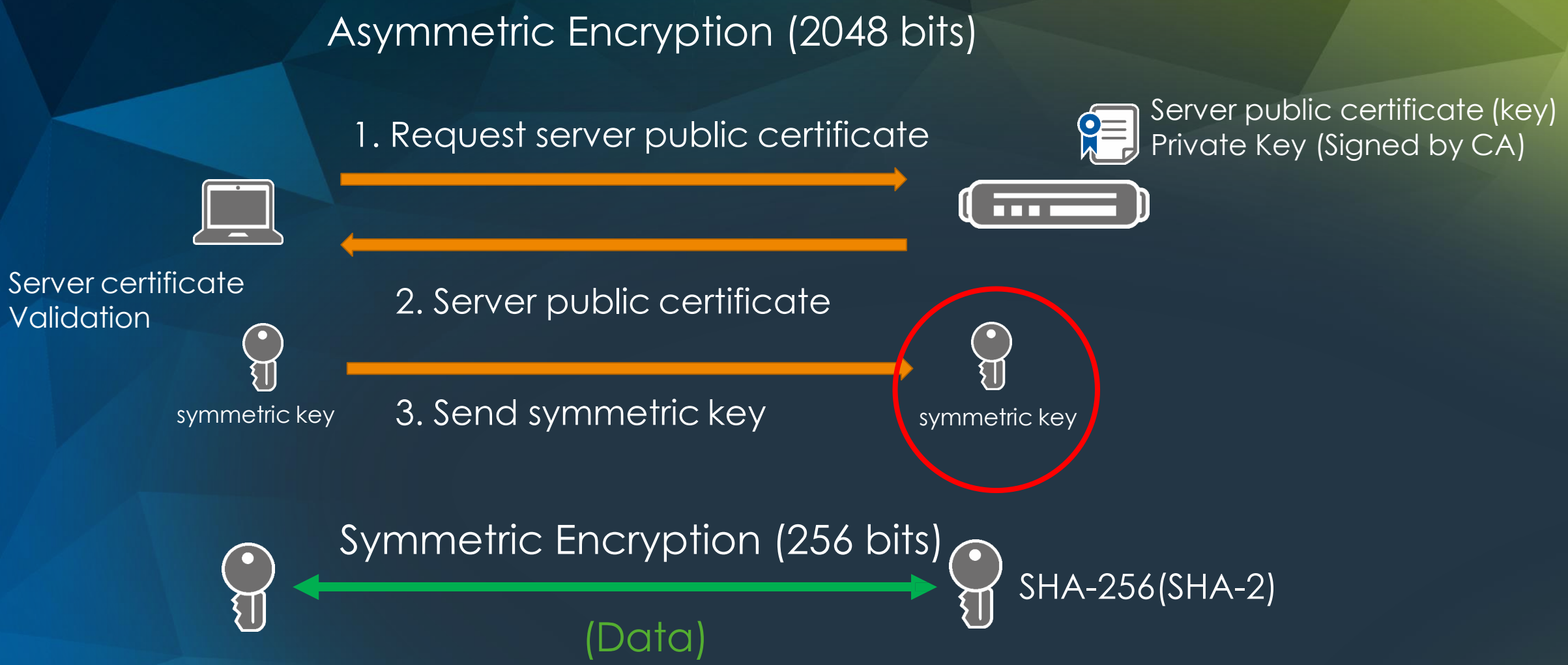
SSL Renegotiation

Server public certificate (key)
Private Key (Signed by CA)

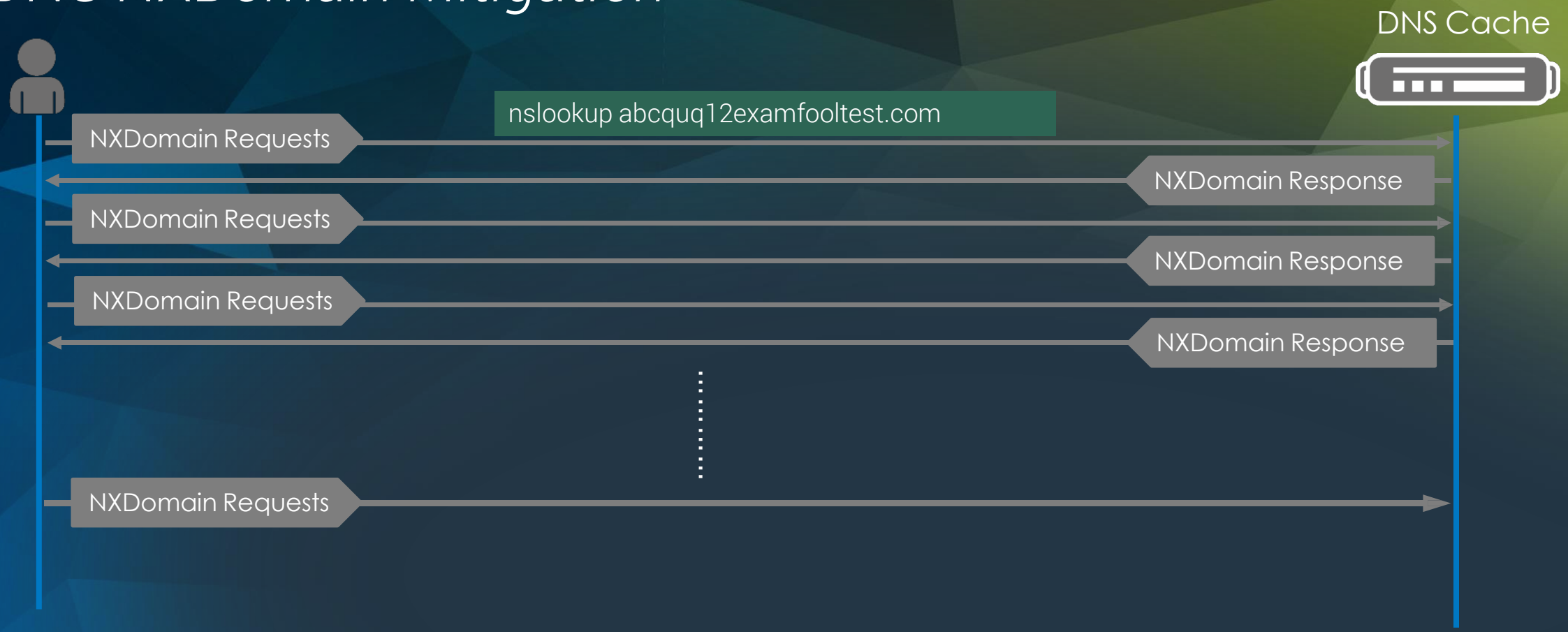




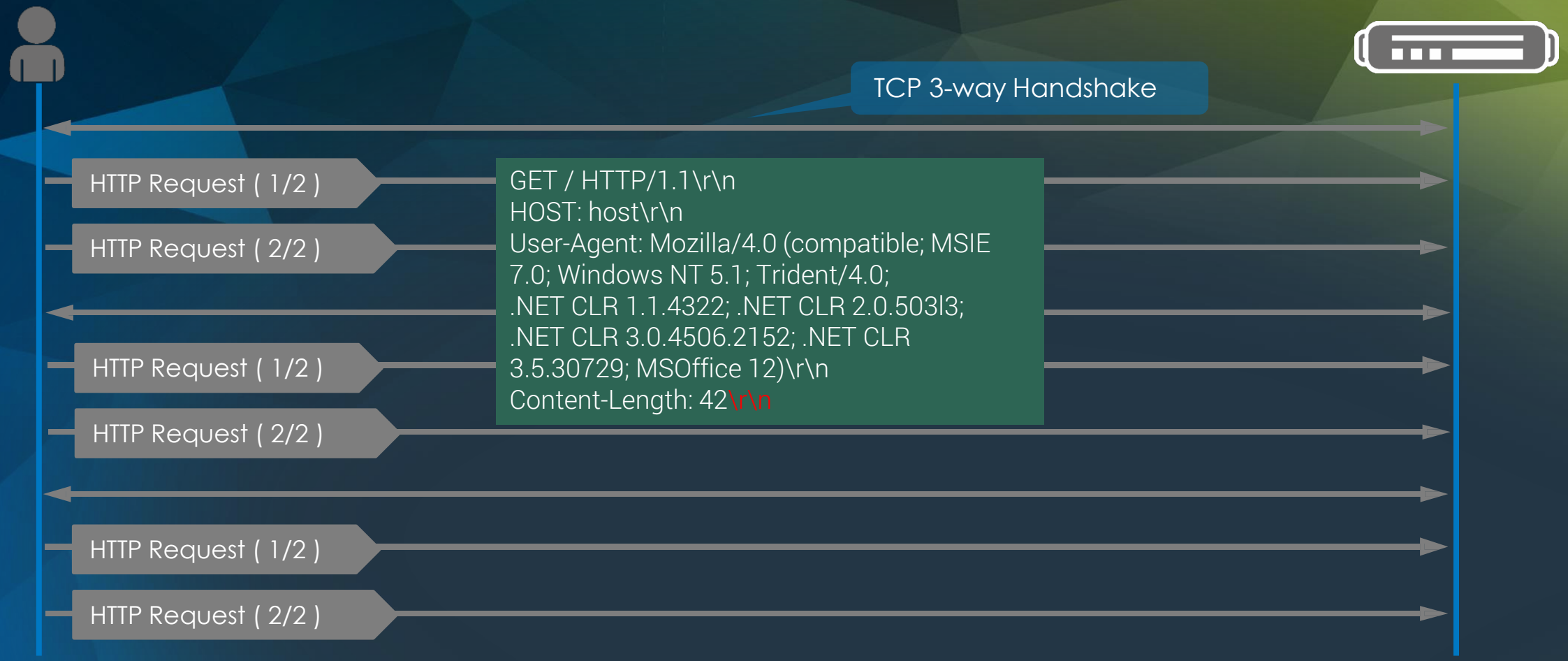
Exploit SSL Handshaking



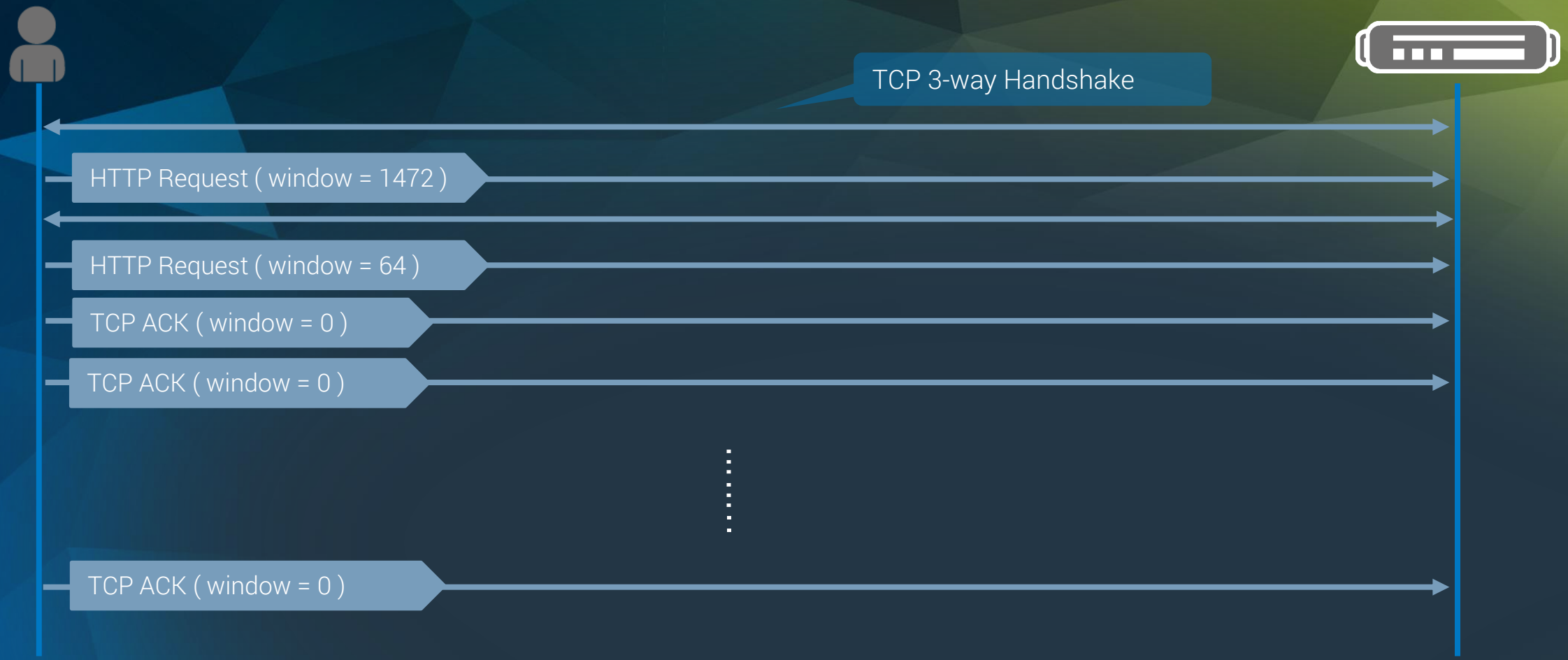
DNS NXDomain Mitigation



HTTP Slowloris

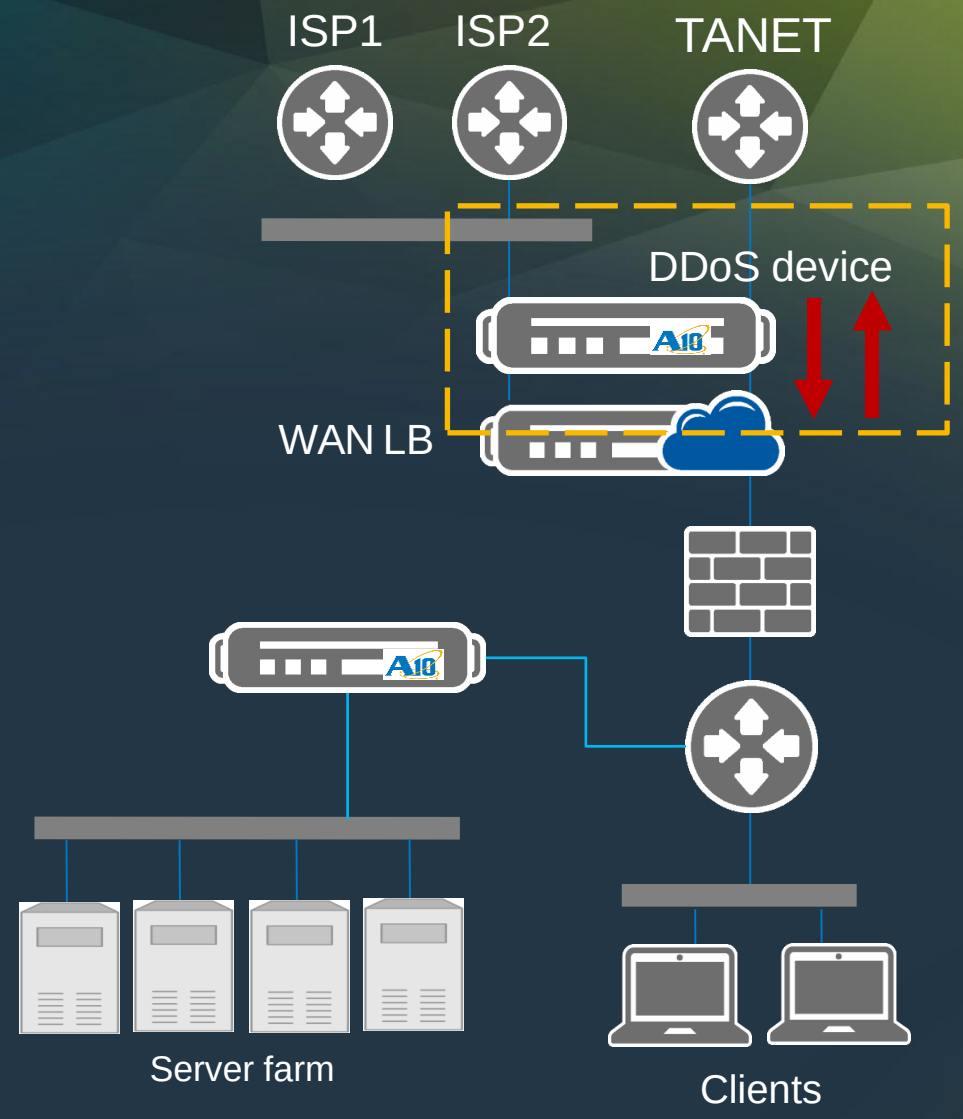


HTTP Slow READ



DDoS 建議防禦架構

- 不只防禦來自校外攻擊
- 同時也要防禦來自校內攻擊
- 防止小流量應用層連線攻擊
- 攻擊發生時自動開啟防禦機制
- 即時紀錄阻擋封包內容



Demo

Q&A

Thank you!