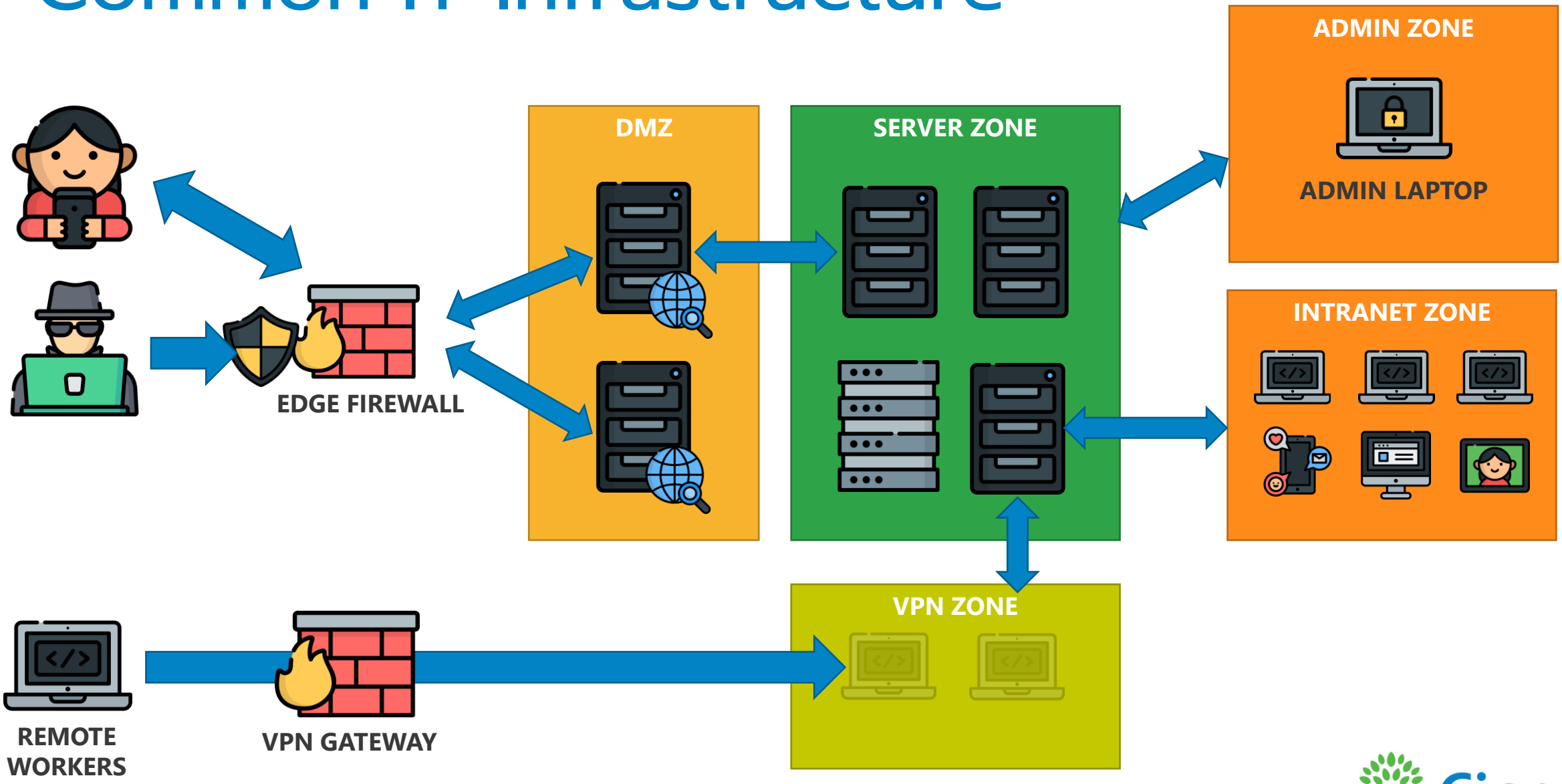
CloudFlare Tunnel

Knowledge Sharing

Cigna®

Common IT Infrastructure



Cigna

Issue

- **Hardware Performance**
  - ตัว Edge Firewall ต้องมีความสามารถในการ Process Package ด้วยความเร็วสูง เพื่อรองรับจำนวนผู้ใช้ที่มากขึ้น ตัวที่เร็วก็ราคาแพง
  - เร็วแค่ไหน ก็ไม่สามารถทน DDoS ไหว
- **Management Overhead**
  - ตามอัพเดท Configuration/OS ของ Firewall ไม่รู้จบ
  - ต้อง **“เจาะ”** ช่อง Firewall ให้ Service เข้าจากภายนอกได้
  - ต้องใช้ Public IP มีค่าใช้จ่ายต่อเดือนเพิ่ม
  - ต้องทำโซน DMZ, แบ่ง VLAN และ Config การ Route ข้ามโซน

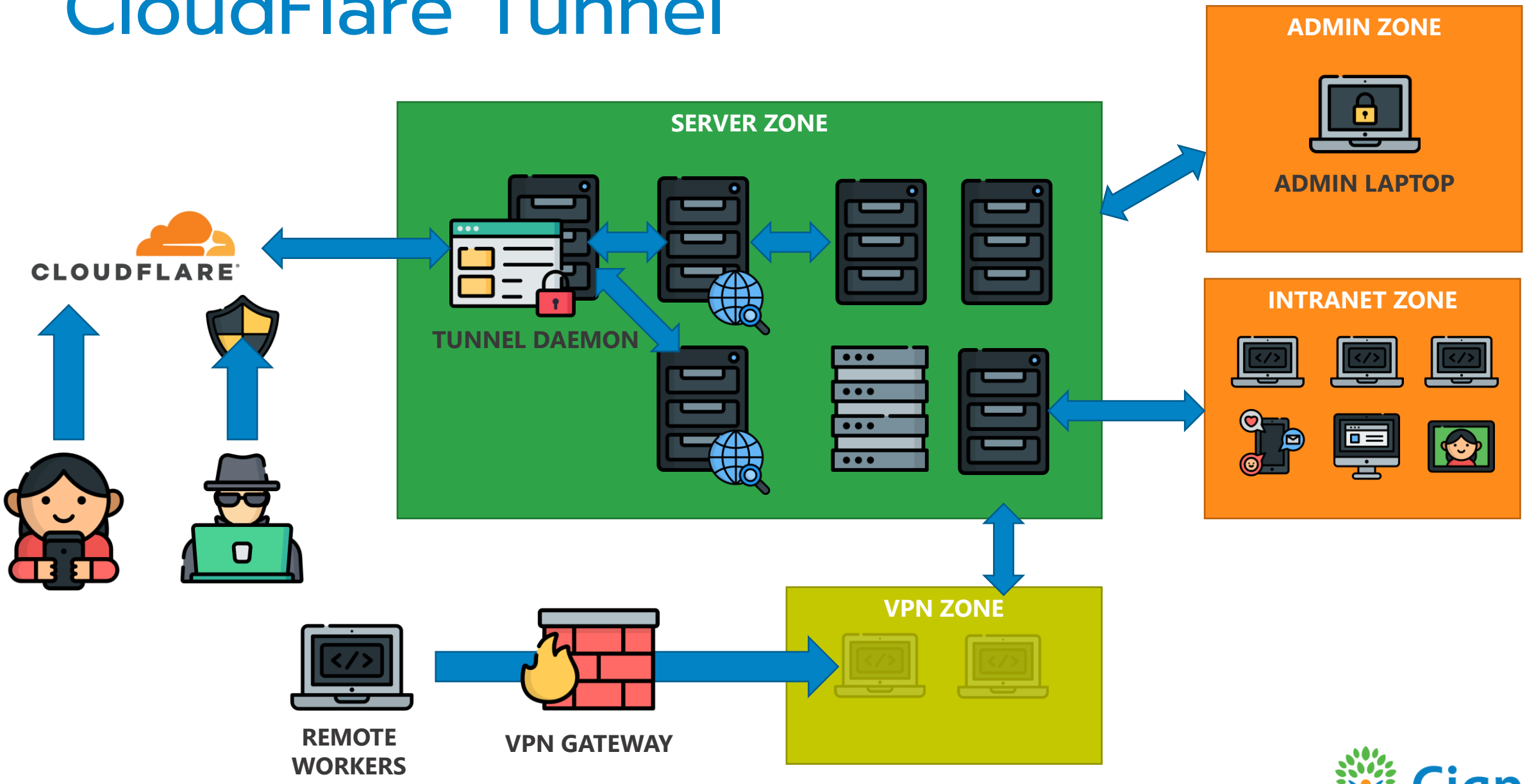
Cigna®

Issue

- **Network Performance**
  - เพื่อป้องกัน Multi-homed Device – Admin จะต้องตั้งให้เครื่องที่ต่อ VPN ออกอินเตอร์เน็ตผ่าน VPN ด้วย ทำให้ทุกเครื่องมา Congest กันที่ Network บริษัท แทนที่กระจายกันได้
  - เพิ่มความซับซ้อนในการตั้งค่า Routing
- **Keys to the Kingdom**
  - คนที่ VPN ได้ ก็เหมือนมีกุญแจเข้า Intranet จากที่ไหนก็ได้

Cigna®

CloudFlare Tunnel



Cigna

Compared to Common Infrastructure

- **ไม่มี DMZ / Forward Port**
  - เพราะไม่มีการ “เจาะ” Firewall
- **ไม่มี Public IP**
  - Routing เกิดภายใน CloudFlare
  - ผู้ที่ต่อเข้ามา มองไม่เห็น IP จริงของฝั่งเรา
- **ไม่มี Edge Firewall ขาเข้า**
  - CloudFlare เป็นด่านหน้า ทำ Filter ให้ทั้งหมด และรับ DDoS ให้

Cigna®

CLIENT

CLOUDFLARE (CF)

TUNNEL DAEMON

SERVICE

เปิด TUNNEL เข้าไปยัง CLOUDFLARE
1 TUNNEL เปิด 4 CONNECTIONS
2 CONNECTIONS ต่อ DATA CENTER
ที่ประเทศไทยจะต่อไป SIN+HK

CLIENT ทำการ QUERY DNS ที่ CF

ได้คำตอบเป็น CNAME ที่ชี้ไปยัง TUNNEL
เช่น WWW -> C52154C3-210B-44CD-8D63-30F49D69D2C5.CFARGOTUNNEL.COM

สามารถทำ Load Balance ที่ CF
เพื่อต่อไปยังหลาย Tunnel ได้

CLIENT REQUEST ไปที่ SERVICE
ARGO TUNNEL

ARGO ROUTE REQUEST เข้า TUNNEL
ส่งเป็น MESSAGE ผ่านโปรโตคอล WEBSOCKET

Tunnel เดียว รวมทุก Service หรือ 1 Tunnel 1 Service ก็ได้
(เปิดจาก Server ที่ Host Service โดยตรง)

TUNNEL DEMON เช็ค HOSTNAME
และทำการแปล MESSAGE ใน WEBSOCKET เป็น
HTTP หรือ TCP ส่งต่อไปยัง SERVER ปลายทาง
และรับคำตอบ

RESPONSE ส่งกลับไปถึง CLIENT

Cigna®

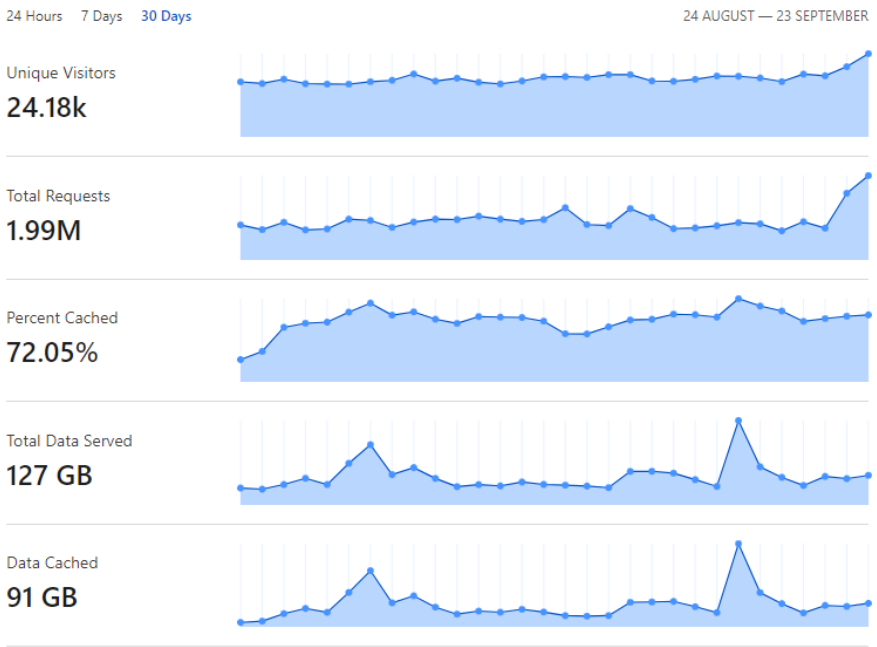
จุดเด่น

- **ฟรี!!!**
  - ก่อนหน้านี้ คิดค่าบริการตาม Bandwidth ที่วิ่งผ่าน Network CF
- **ไม่มีการ Config Firewall / VLAN / ZONE**
  - เพราะไม่มีการ “เจาะ” Firewall จึงไม่ต้องทำ Zone และจึงไม่มีการ Route ข้าม Zone ลดจำนวน Configuration ที่ต้องจัดการ
- **Offload งาน Packet Filter ไปที่ CloudFlare ทั้งหมด**
  - ไม่ต้องลงทุน Hardware Firewall / License
  - ประสิทธิภาพสูงกว่า Hardware ที่ซื้อเอง (Network CloudFlare อยู่ที่ 90Tbps)

Cigna®

จุดเด่น

- **ประหยัดค่า Cloud Server / Bandwidth**
  - ไม่ต้องเสียค่าเช่า Server สามารถตั้ง Server On-Premises ได้ทั้งหมด โดยได้ประสิทธิภาพเหมือน Cloud
  - CloudFlare จะทำการ Cache ให้ด้วย สำหรับเคส Reverse Proxy ประหยัด Bandwidth – ใช้ Bandwidth เฉพาะ API Request/HTML เท่านั้น Resource อื่นๆ สามารถ Cache ได้ทั้งหมด



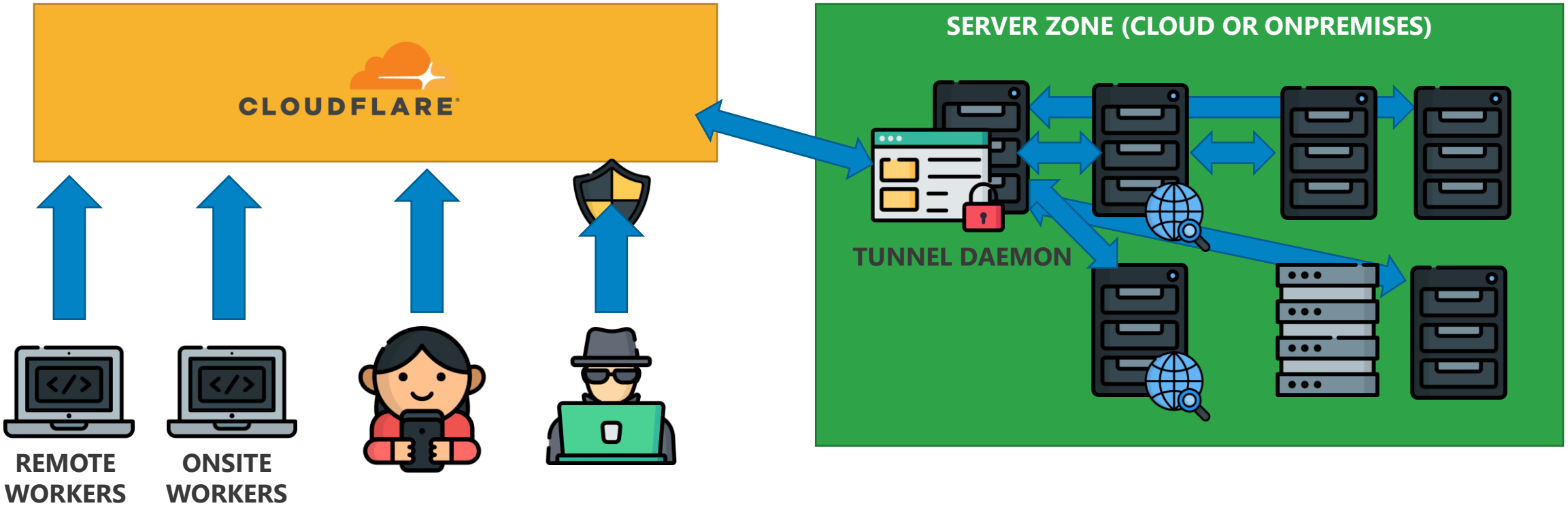
จุดเด่น

- **ถ้าต้องการ Reverse SSH/RDP/TCP ต้องใช้ Tunnel Client**
  - ไม่สามารถใช้ Client ต่อโดยตรงได้ บังคับให้ CloudFlare Filter ให้ก่อน

- **ประหยัดค่า SSL Cert และไม่ต้องดูแล Cert เอง**
  - CloudFlare เป็นตัว Offload SSL ให้ทั้งหมด
  - SSL Cert ใช้ Wildcard Cert ของ CloudFlare ซึ่งต่ออายุอัตโนมัติ

Cigna®

CloudFlare For Teams (+Zero Trust)



จุดเด่น

- **Support Work from Anywhere / BYOD**
  - Authenticate ด้วย 3rd Party ได้ เช่น OKTA, Facebook, Google, Microsoft, Azure AD
  - ไม่ต้องมี VPN แล้ว และ CloudFlare เป็นคนจำกัดสิทธิ์การเข้า Server แทน
- **ไม่ต้องลงทุน Bandwidth เพิ่มเพื่อรองรับ Remote Work**
  - Traffic ออกอินเตอร์เน็ต (เช่น WebEx Meeting) ภายใน Office สามารถใช้แบบ Consumer ได้
  - สามารถ Log Traffic / Block Traffic อินเตอร์เน็ต ที่ CloudFlare ได้

Cigna®

RISK

- **Single Point of Control / Single Point of Failure**
  - CloudFlare อาจเกิด Service Disruption ได้
  - ไม่สามารถย้ายไป Vendor อื่นได้ง่าย ปัจจุบันยังไม่มีคู่แข่ง

- **Bait and Switch**
  - หลังมีผู้ใช้งานมาก อาจเรียกเก็บค่าบริการ
    - แต่อาจไม่เกิดขึ้น เนื่องจากเคยเป็นบริการที่เสียเงิน และเป็นช่องทางที่ปลอดภัยกว่าสำหรับ CloudFlare ในการยืนยันตัว Origin Server ว่าเป็นของ Domain นั้นจริง (https://qt.gy/post/2021-8-26-bypassing-cloudflare-using-cloudflare)

Cigna

Q&A

Cigna®