An toàn bảo mật trên nền IPv6-Only: Kiểm soát, bảo vệ lưu lượng mạng và truy vấn DNS

Nguyen Thanh Bien

Principal Solution Engineer – F5

Nội dung

- Mở đầu
- IPv6 firewall
- An toàn – bảo mật cho DNS
- S/Gi Firewall tích hợp đa dịch vụ

Tỷ lệ chuyển đổi IPv6 (2020 – 2025)

Năm	Tỷ lệ sử dụng IPv6 toàn quốc	Ghi chú
2020	~40%	Bắt đầu chương trình chuyển đổi số quốc gia
2021	45%	Hơn 34 triệu người dùng IPv6
2023	53%	Tăng trưởng ổn định hạ tầng băng rộng và di động
2024	65.5%	Vượt 1.6 lần trung bình toàn cầu
2025	67% – 70%	Chuẩn bị sang IPv6-only

Hiện trạng hạ tầng hỗ trợ IPv6

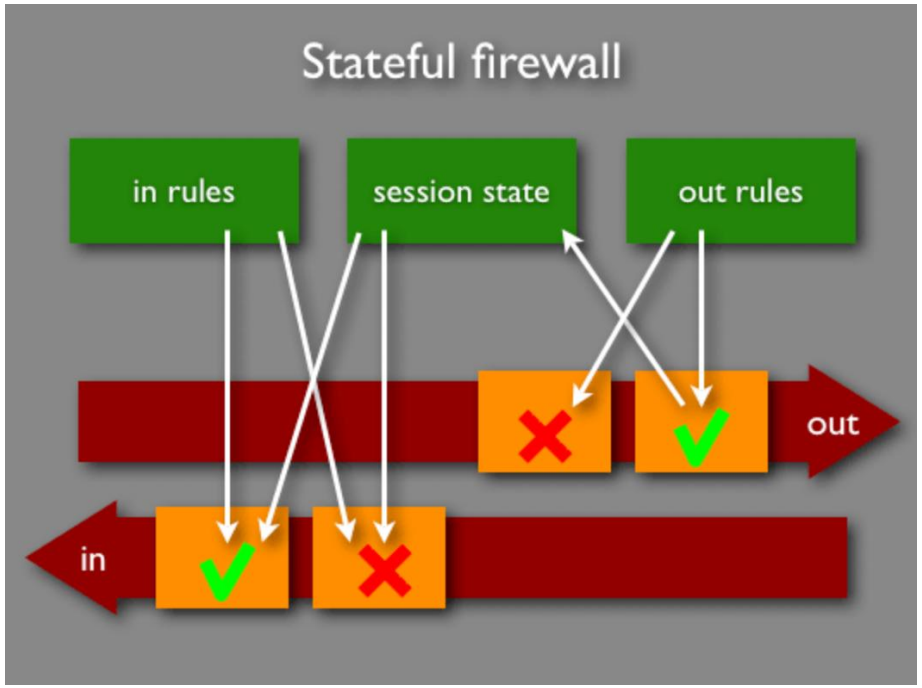
- **Thuê bao**
  - Cố định/băng rộng: 80% - 82%
  - Di động: 83% - 88%
- **Các nhà mạng**
  - MobiFone: ~76%
  - FPT Telecom: ~67%
  - Viettel: ~65%
  - VNPT: ~53%
- **Lộ trình “IPv6 only”**
  - 2026 – 2028: chỉ sử dụng IPv4 cho các hệ thống đặc thù, thí điểm IPv6 only
  - 2029 – 2030: đạt tỷ lệ 90%-100%, đồng bộ IPv6-only trên toàn quốc
  - Đến 2032: ngưng sử dụng IPv4

Rủi ro bảo mật khi mọi thiết bị đều có địa chỉ IPv6

- Mất lớp bảo vệ NAT (Network Address Translation), mọi thiết bị đều “phơi” trực tiếp
- Dễ quét port hơn
- Rủi ro với các thiết bị IoT, smart devices, hệ thống nhúng
- Rủi ro với tấn công DDOS
- IPv6 với IPsec chuyển từ “bắt buộc” sang “khuyến nghị”:
  - Thiết bị IoT có cấu hình thấp
  - Quản lý khóa phức tạp trên quy mô lớn
  - Sự phổ biến của mã hóa “tầng trên”: SSL/TLS, SSH…

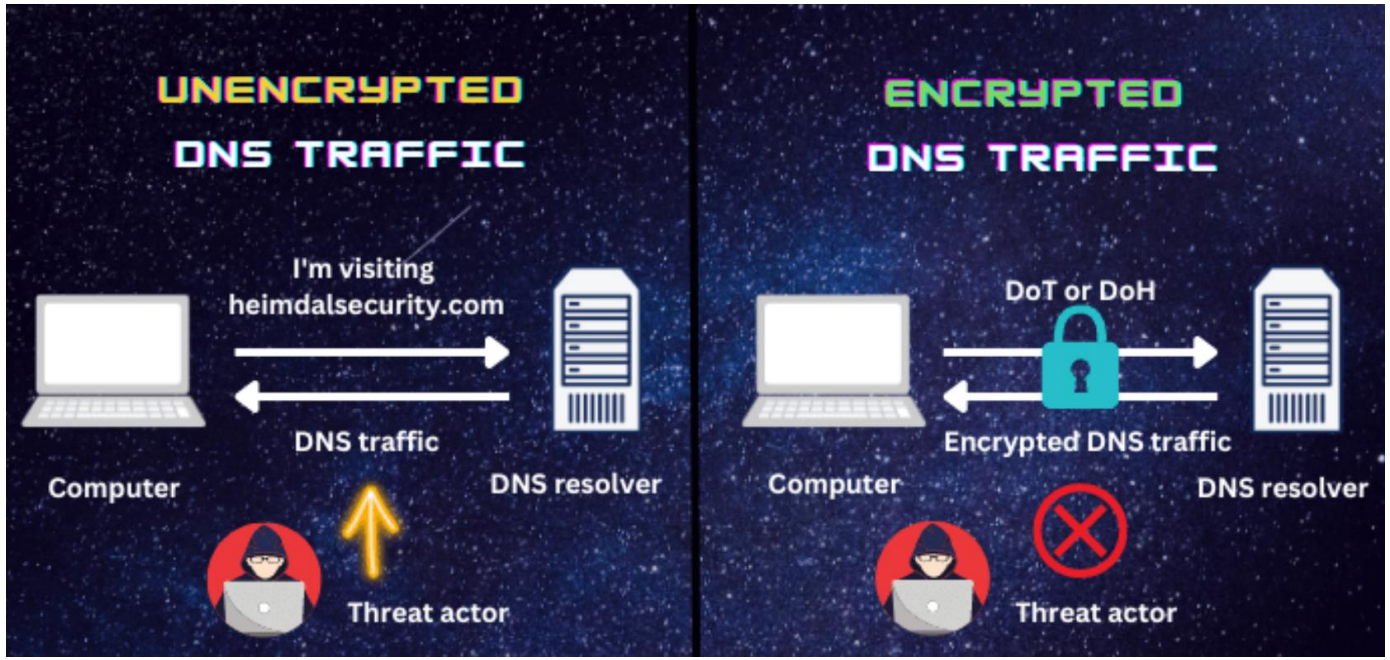
IPv6 firewall

- Default deny
- Stateful firewall
- Hỗ trợ ICMPv6 cần thiết:
  - Neighbor Discovery (ND)
  - Router Advertisements (RA)
- Chống tấn công DDOS



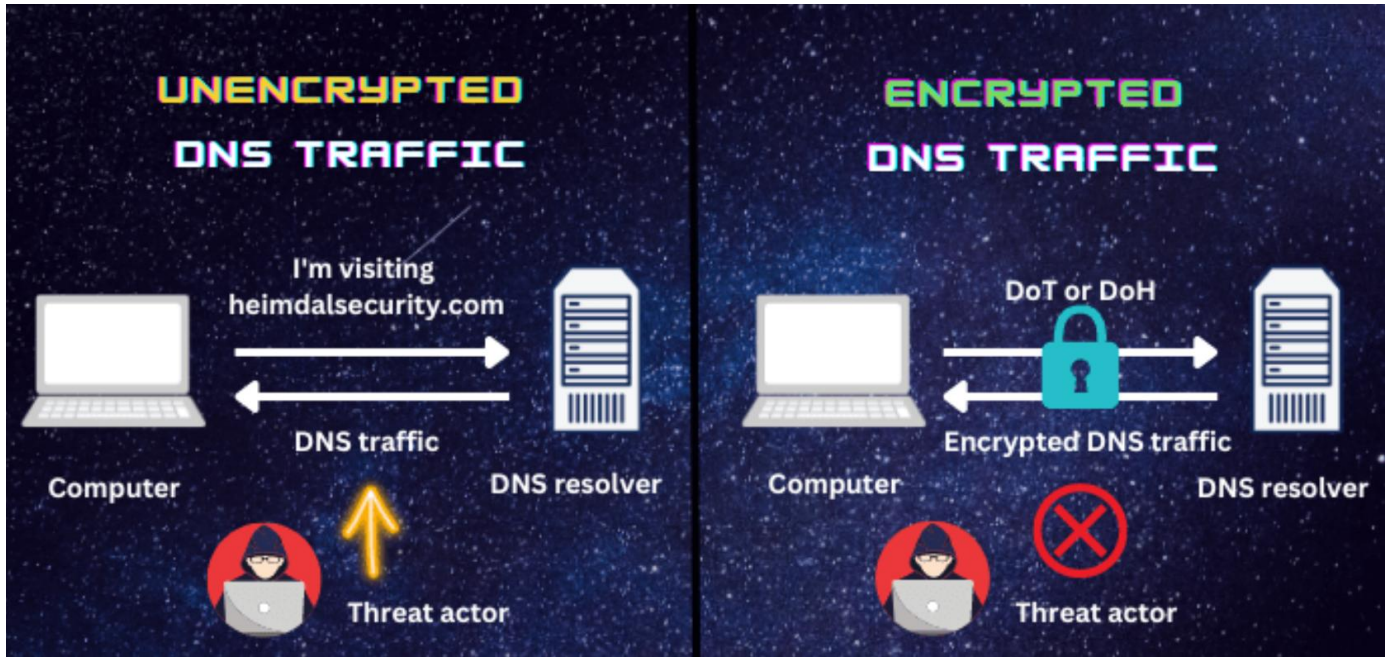
An toàn – bảo mật cho DNS

- Hơn 4 thập kỷ phát triển
- “Clear-text” DNS (tcp/udp 53)
- DNSSEC
- “Encrypted” DNS:
  - DoT
  - DoH
  - ODoH
- DNS64/NAT64

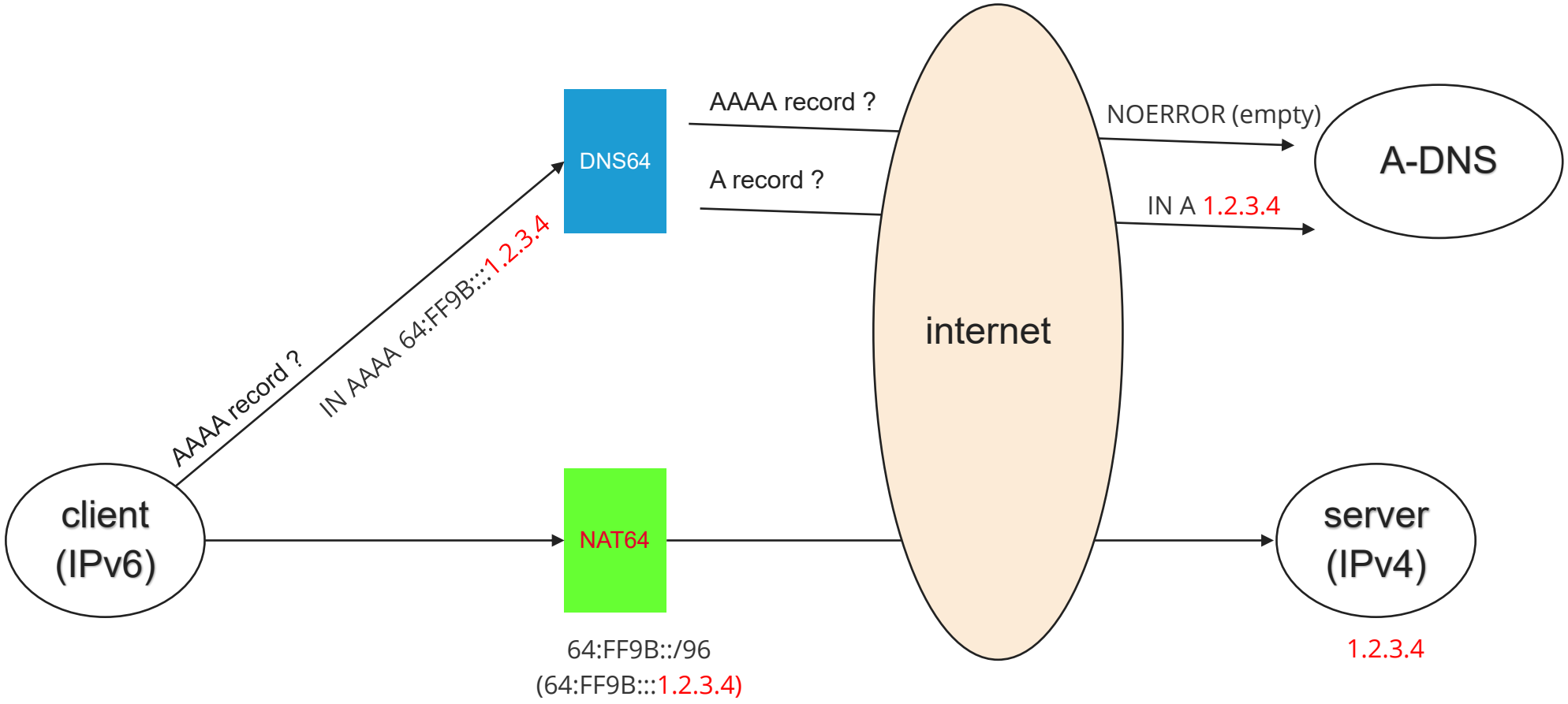


An toàn – bảo mật cho DNS

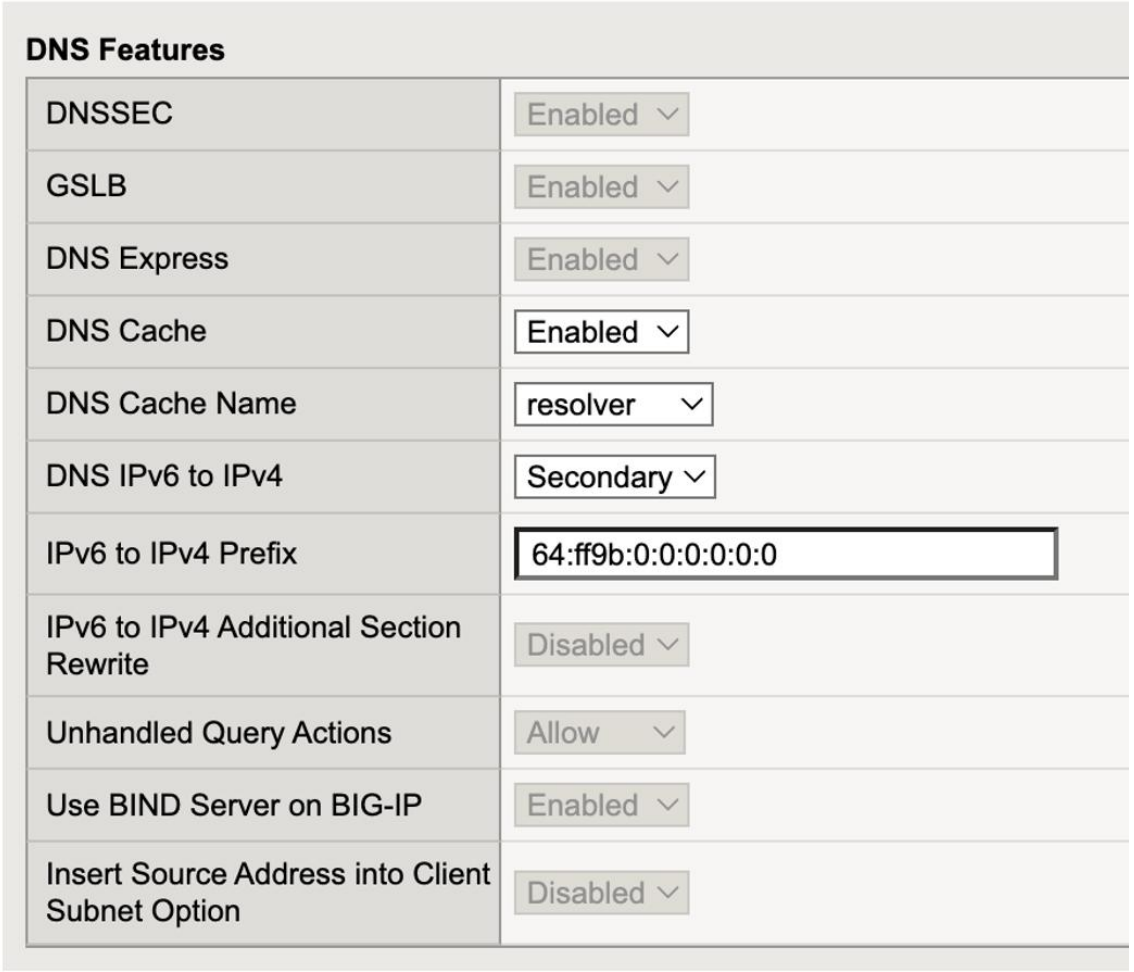
- Hơn 4 thập kỷ phát triển
- “Clear-text” DNS (tcp/udp 53)
- DNSSEC
- “Encrypted” DNS:
  - DoT
  - DoH
  - ODoH
- DNS64/NAT64



Supporting DNS64 – F5 BIG-IP



Supporting DNS64 – F5 BIG-IP

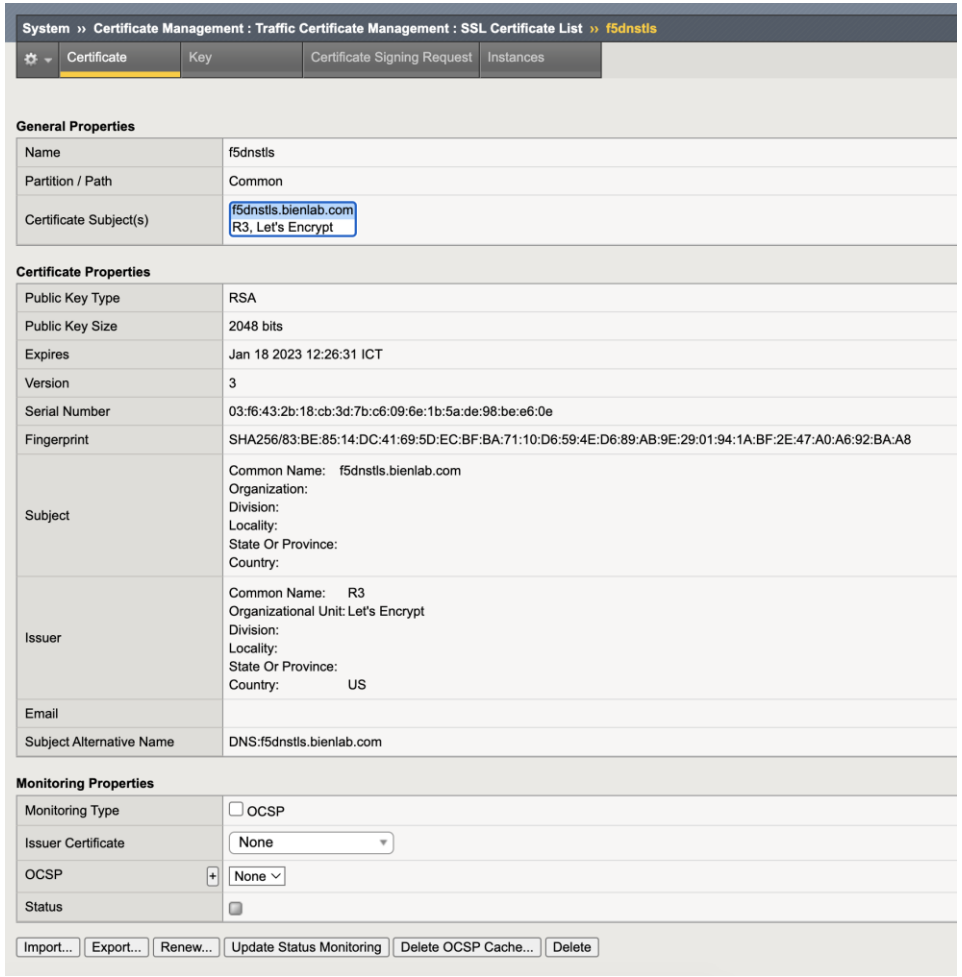


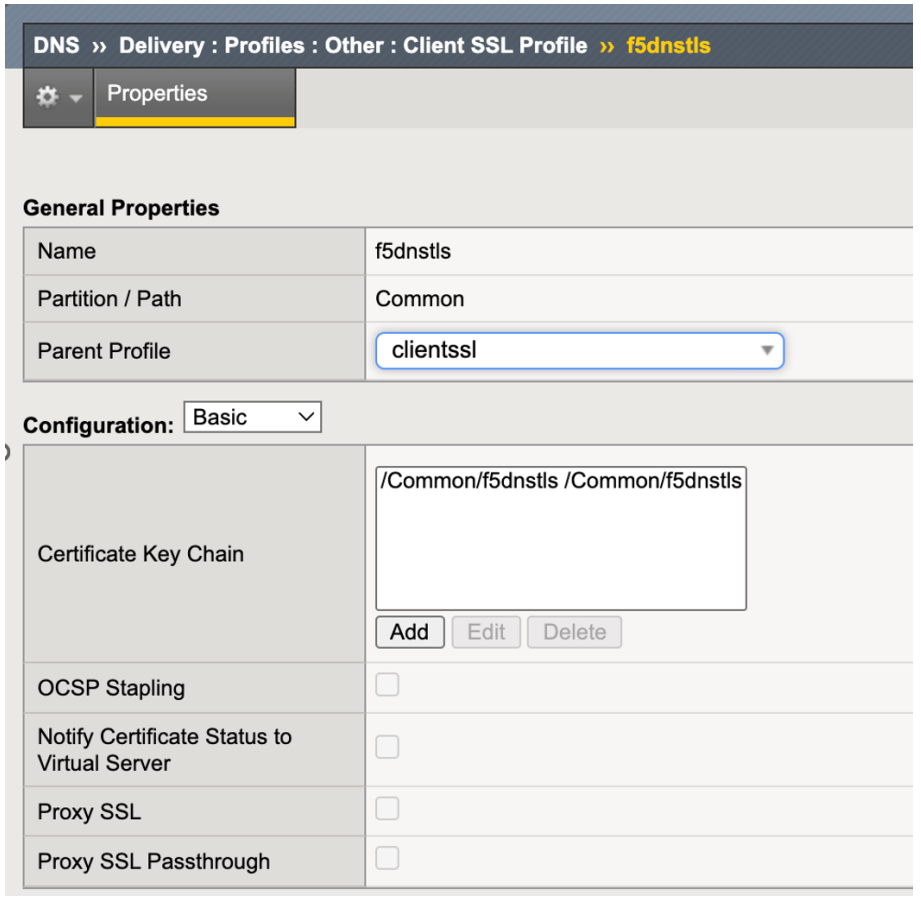
Supporting DNS64 – F5 BIG-IP

```
ubuntu@i-0c62052040efaf8e8:~$ dig @2406:da1e:804:8a00:3437:36:ebfc:5a18 f5dnsv4.bienlab.com AAAA

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> @2406:da1e:804:8a00:3437:36:ebfc:5a18 f5dnsv4.bienlab.com
AAAA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44769
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;f5dnsv4.bienlab.com.           IN      AAAA

;; ANSWER SECTION:
f5dnsv4.bienlab.com.    300     IN      AAAA    64:ff9b::10a2:fee5

;; Query time: 140 msec
;; SERVER: 2406:da1e:804:8a00:3437:36:ebfc:5a18#53(2406:da1e:804:8a00:3437:36:ebfc:5a18) (UDP)
;; WHEN: Tue Nov 01 06:43:38 UTC 2022
;; MSG SIZE  rcvd: 76
```

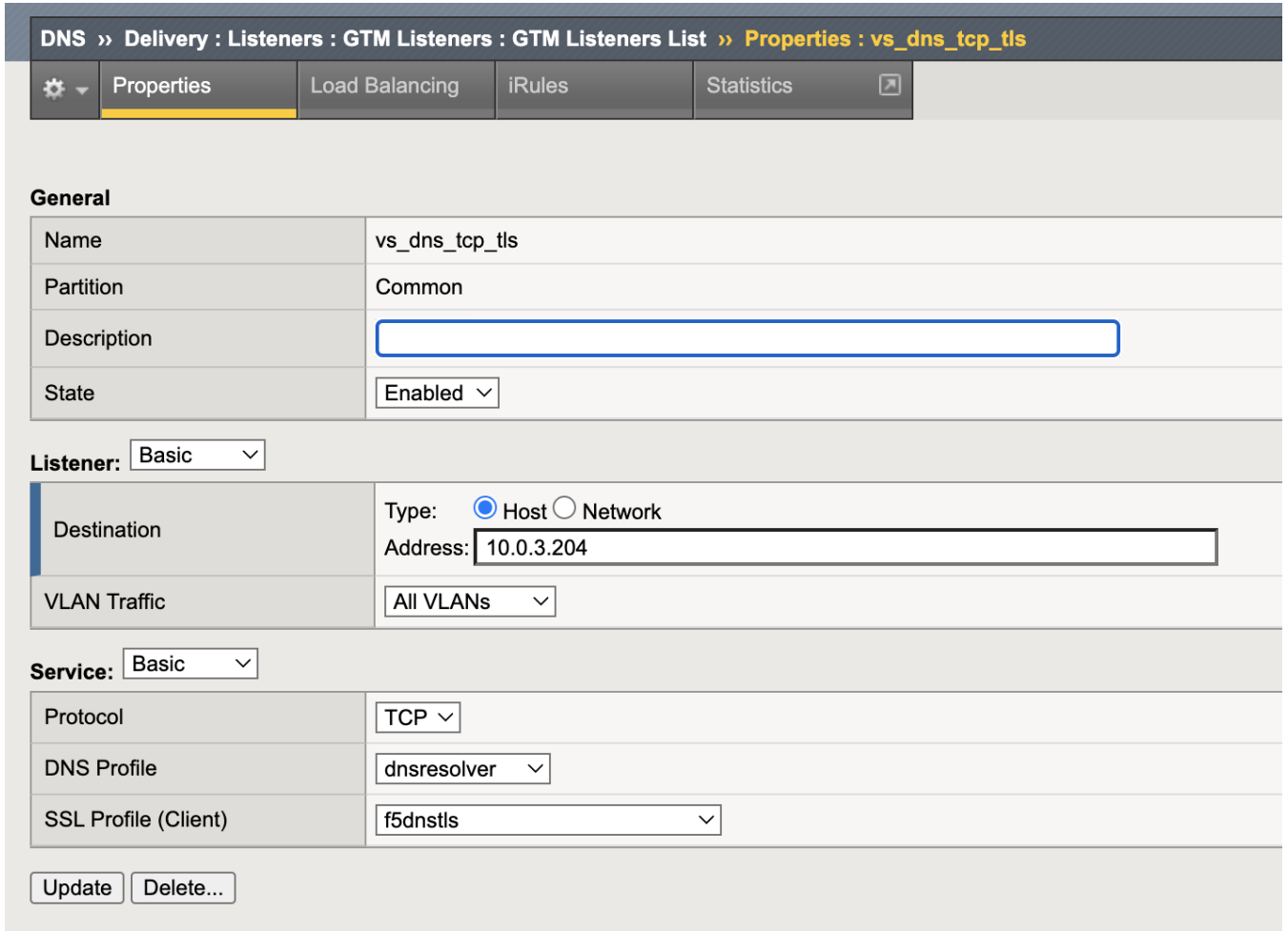
64:ff9b:0:0:0:0:0:0 16.162.254.229

Supporting DOT (DNS over TLS) – F5 BIG-IP

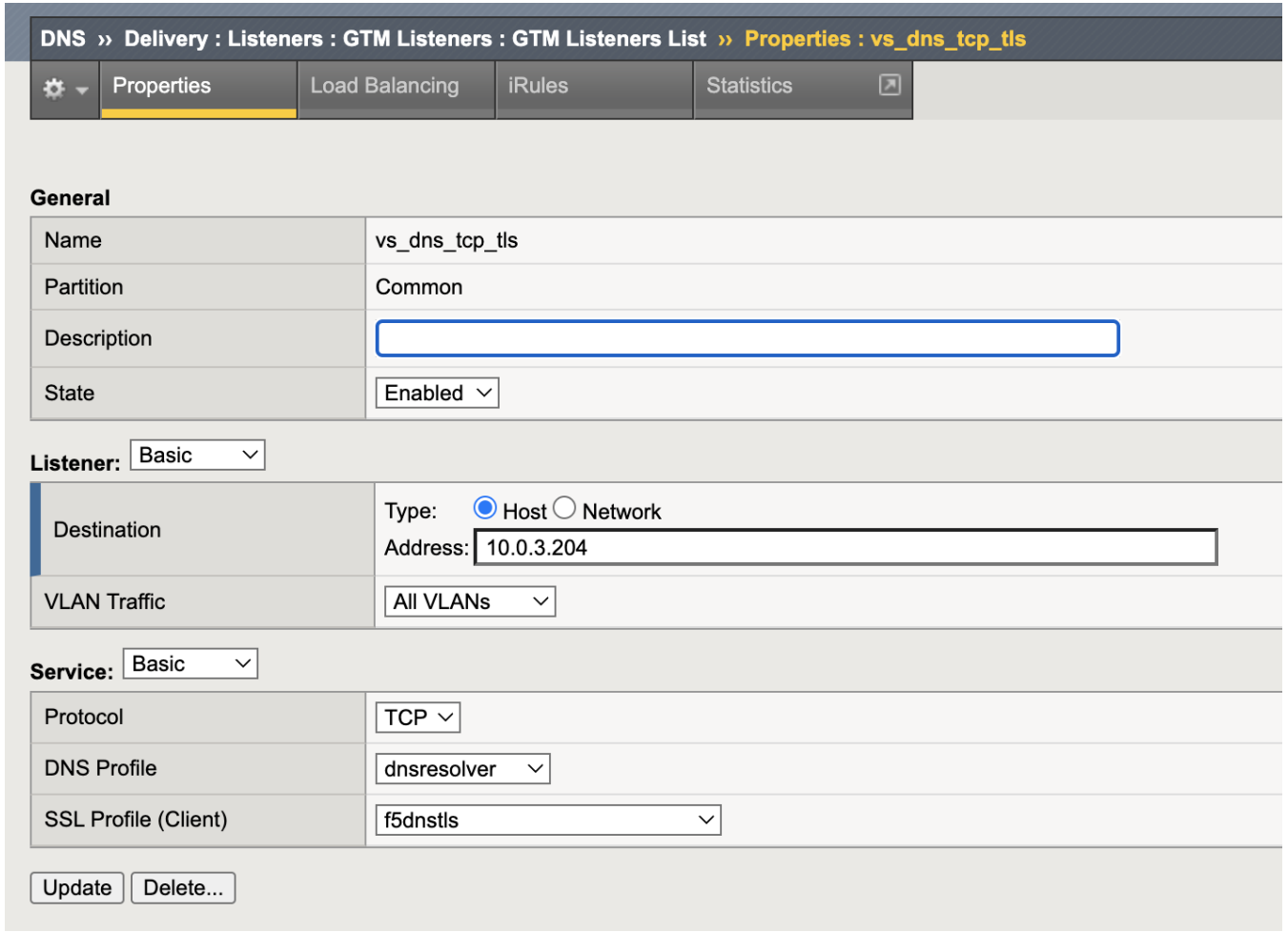




Supporting DOT (DNS over TLS) – F5 BIG-IP



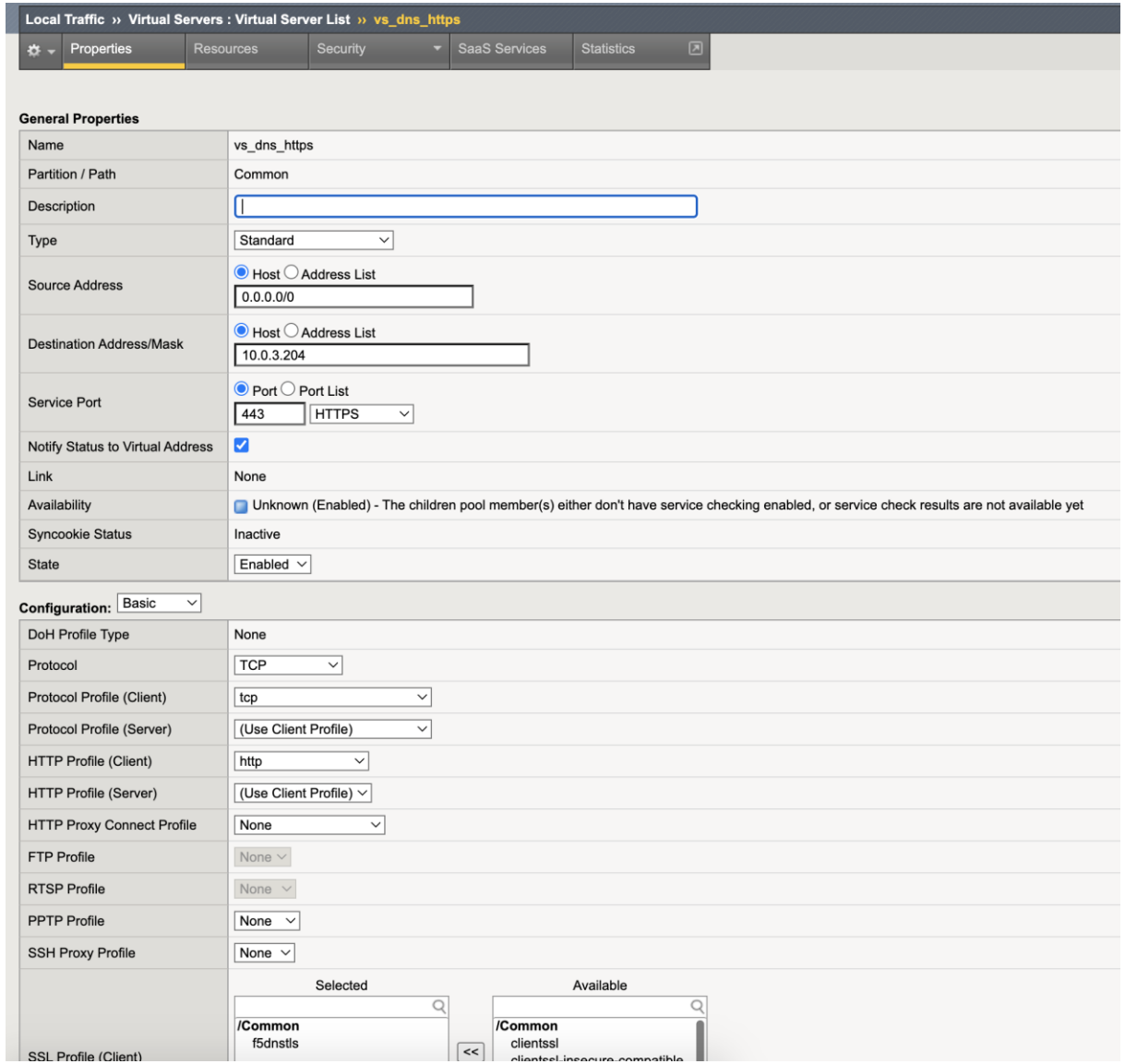
Supporting DOT (DNS over TLS) – F5 BIG-IP



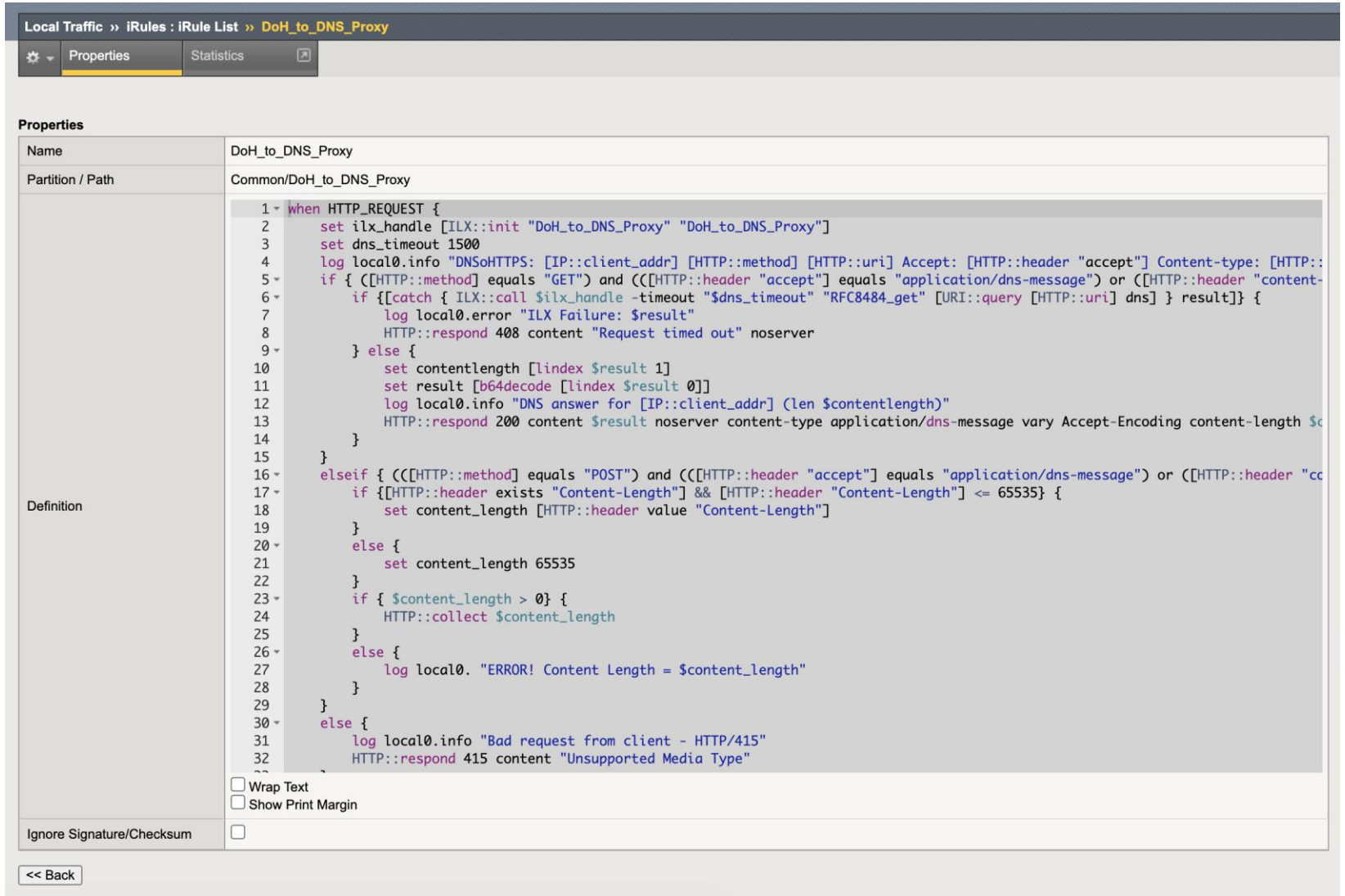
Supporting DOT (DNS over TLS) – F5 BIG-IP

```
ubuntu@i-0c62052040efaf8e8:~$ kdig @10.0.3.204 +tls vnexpress.net
;; TLS session (TLS1.2)-(ECDHE-SECP256R1)-(RSA-SHA256)-(AES-128-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 15661
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 2; ADDITIONAL: 1

;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 4096 B; ext-rcode: NOERROR

;; QUESTION SECTION:
;; vnexpress.net.               IN      A

;; ANSWER SECTION:
vnexpress.net.          296     IN      A       111.65.250.2

;; AUTHORITY SECTION:
vnexpress.net.          296     IN      NS      ns1.fptonline.vn.
vnexpress.net.          296     IN      NS      ns2.fptonline.vn.

;; Received 106 B
;; Time 2022-11-01 06:57:40 UTC
;; From 10.0.3.204@853(TCP) in 0.9 ms
```

Supporting DOH (DNS over HTTPS) – F5 BIG-IP



Supporting DOH (DNS over HTTPS) – F5 BIG-IP



Supporting DOH (DNS over HTTPS) – F5 BIG-IP

Mozilla Firefox

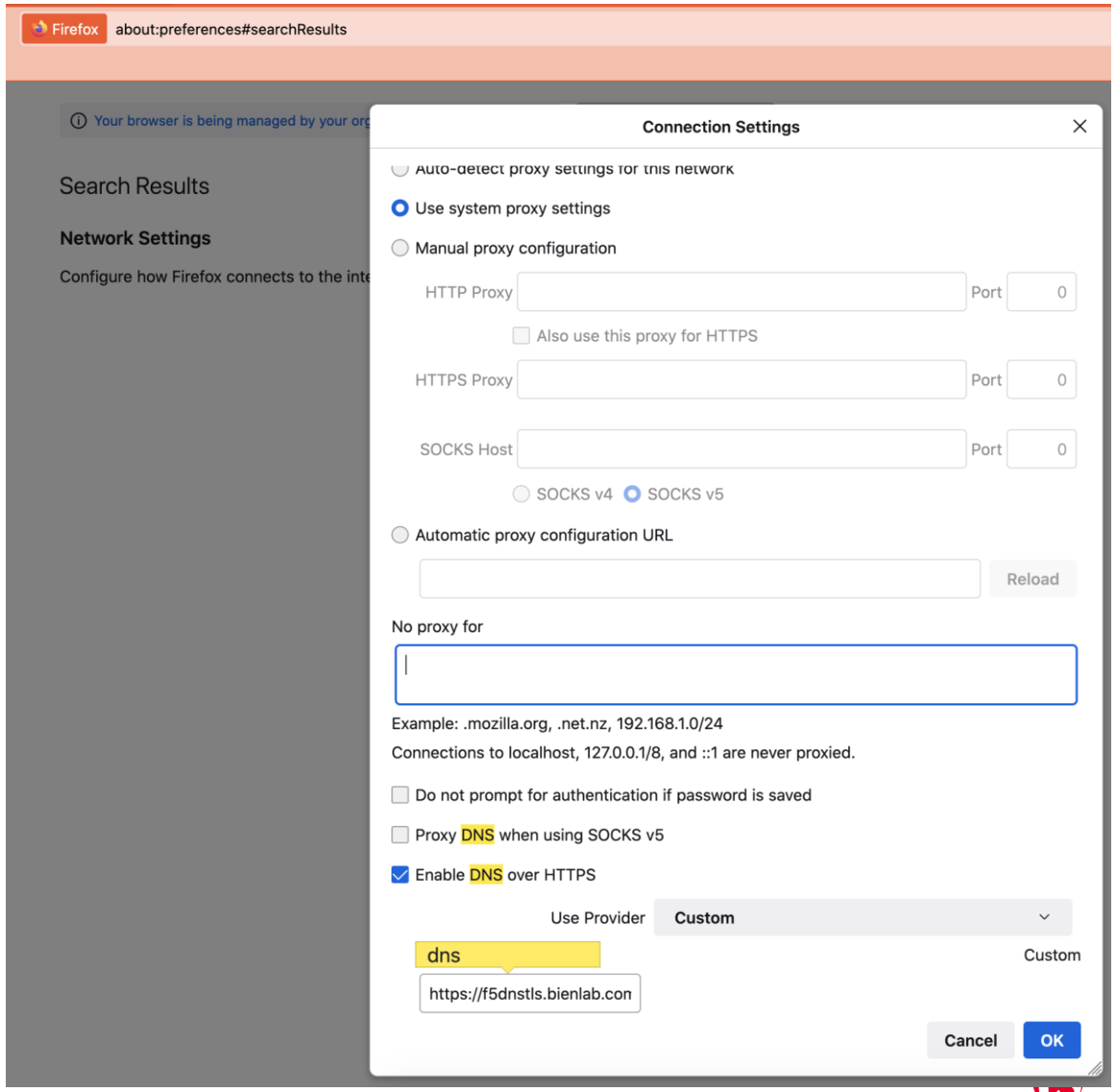
1. Select the menu button > **Settings**.
2. In the **General** menu, scroll down to access **Network Settings**.
3. Select **Settings**.
4. Select **Enable DNS over HTTPS**. By default, it resolves to Cloudflare DNS.

Google Chrome

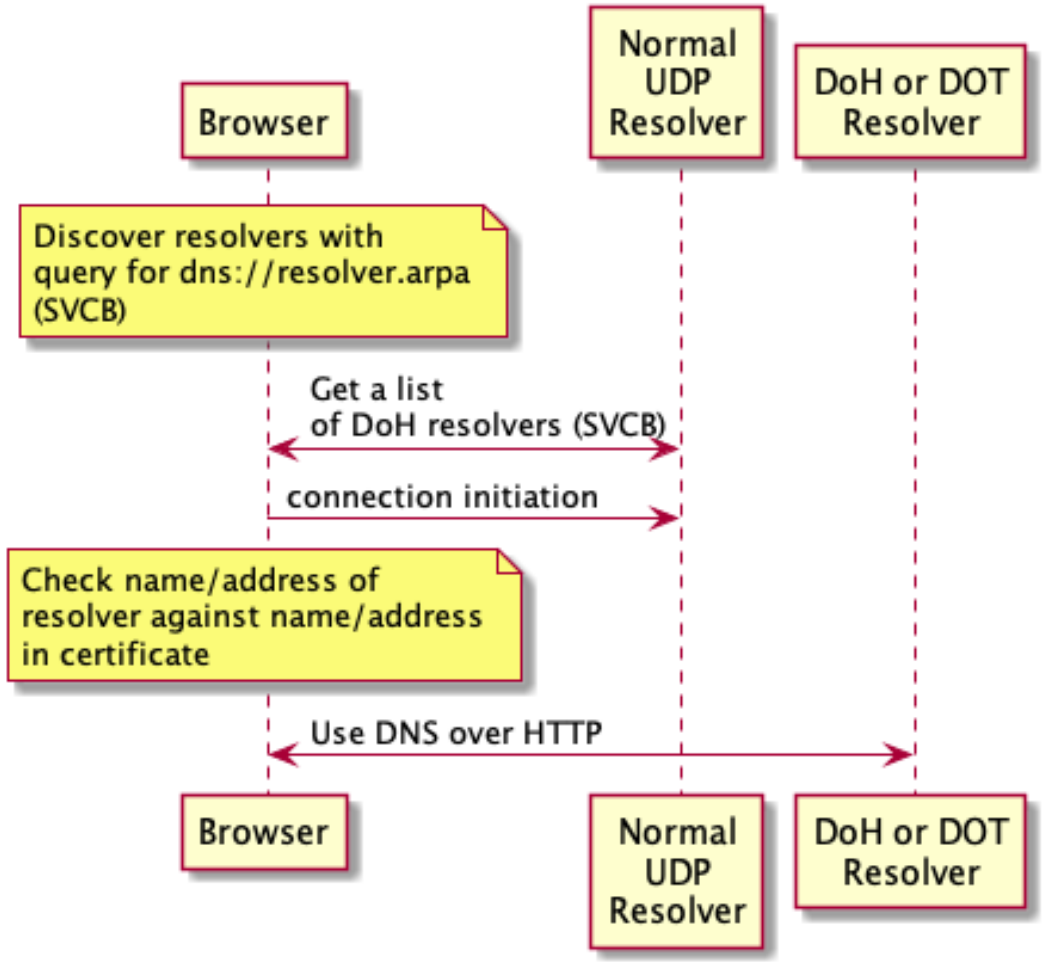
1. Select the three-dot menu in your browser > **Settings**.
2. Select **Privacy and security** > **Security**.
3. Scroll down and enable **Use secure DNS**.
4. Select the **With** option, and from the drop-down menu choose *Cloudflare (1.1.1.1)*.

Microsoft Edge

1. Select the three-dot menu in your browser > **Settings**.
2. Select **Privacy, Search, and Services**, and scroll down to **Security**.
3. Enable **Use secure DNS**.
4. Select **Choose a service provider**.
5. Select the **Enter custom provider** drop-down menu and choose *Cloudflare (1.1.1.1)*.



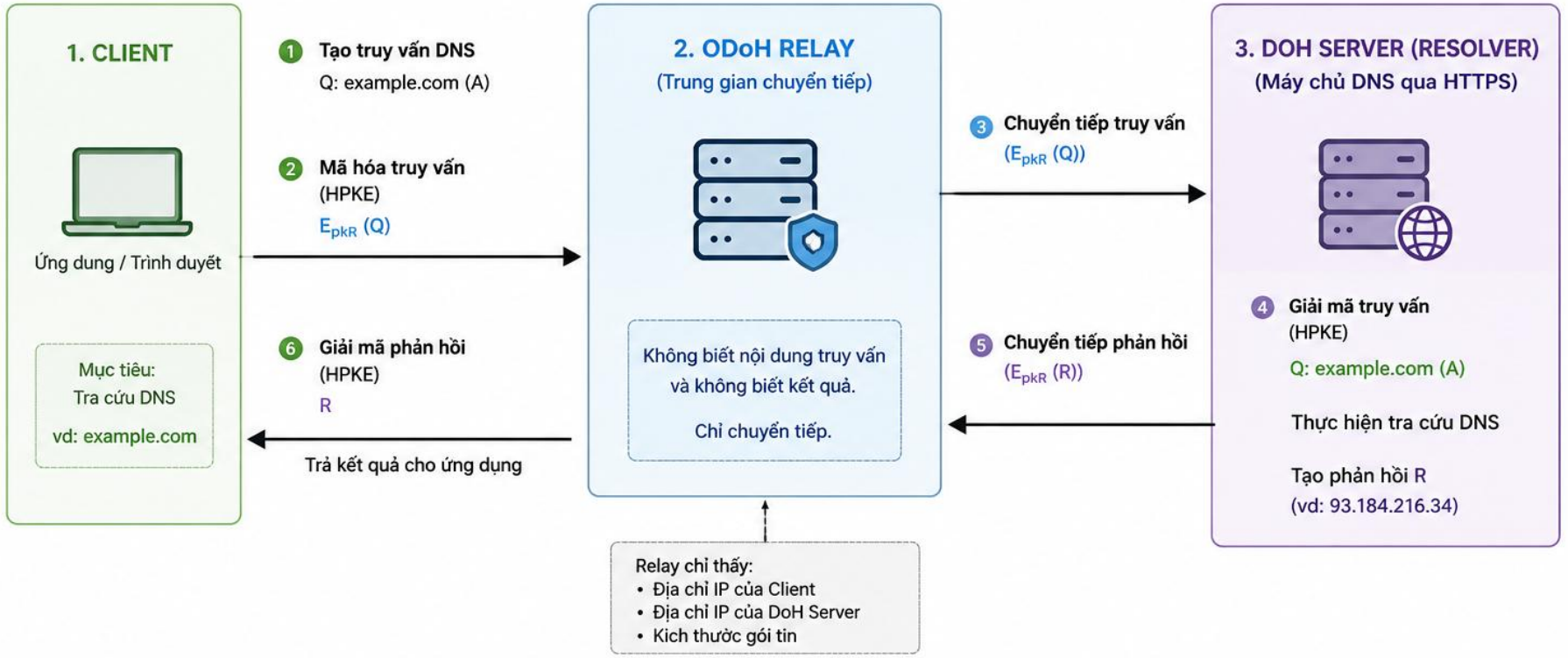
_dns.resolver.arpa (SVCB record)



_dns.resolver.arpa (SVCB record)

```
bien@bienlab:~$ dig @8.8.8.8 _dns.resolver.arpa svcb

; <<>> DiG 9.18.39-0ubuntu0.24.04.5-Ubuntu <<>> @8.8.8.8 _dns.resolver.arpa svcb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4874
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 4

;; QUESTION SECTION:
;_dns.resolver.arpa.            IN      SVCB

;; ANSWER SECTION:
_dns.resolver.arpa.     86400   IN      SVCB    1 dns.google. alpn="dot"
_dns.resolver.arpa.     86400   IN      SVCB    2 dns.google. alpn="h2,h3" key7="/dns-query{?dns}"

;; ADDITIONAL SECTION:
dns.google.             86400   IN      A       8.8.8.8
dns.google.             86400   IN      A       8.8.4.4
dns.google.             86400   IN      AAAA    2001:4860:4860::8888
dns.google.             86400   IN      AAAA    2001:4860:4860::8844

;; Query time: 20 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Thu Jun 11 21:55:04 +07 2026
;; MSG SIZE  rcvd: 224
```

SƠ ĐỒ HOẠT ĐỘNG ODoH
(Oblivious DoH)



LUỒNG HOẠT ĐỘNG TÓM TẮT

1. Client tạo truy vấn DNS Q.
2. Client mã hóa Q bằng khóa công khai của Relay.
3. Relay chuyển tiếp truy vấn đã mã hóa tới DoH Server.
4. DoH Server giải mã, xử lý truy vấn và tạo phản hồi R.
5. DoH Server mã hóa phản hồi bằng khóa công khai của Relay và gửi lại cho Relay.
6. Relay chuyển tiếp phản hồi đã mã hóa về cho Client.
7. Client giải mã phản hồi và trả kết quả cho ứng dụng.

TÍNH CHẤT BẢO MẬT

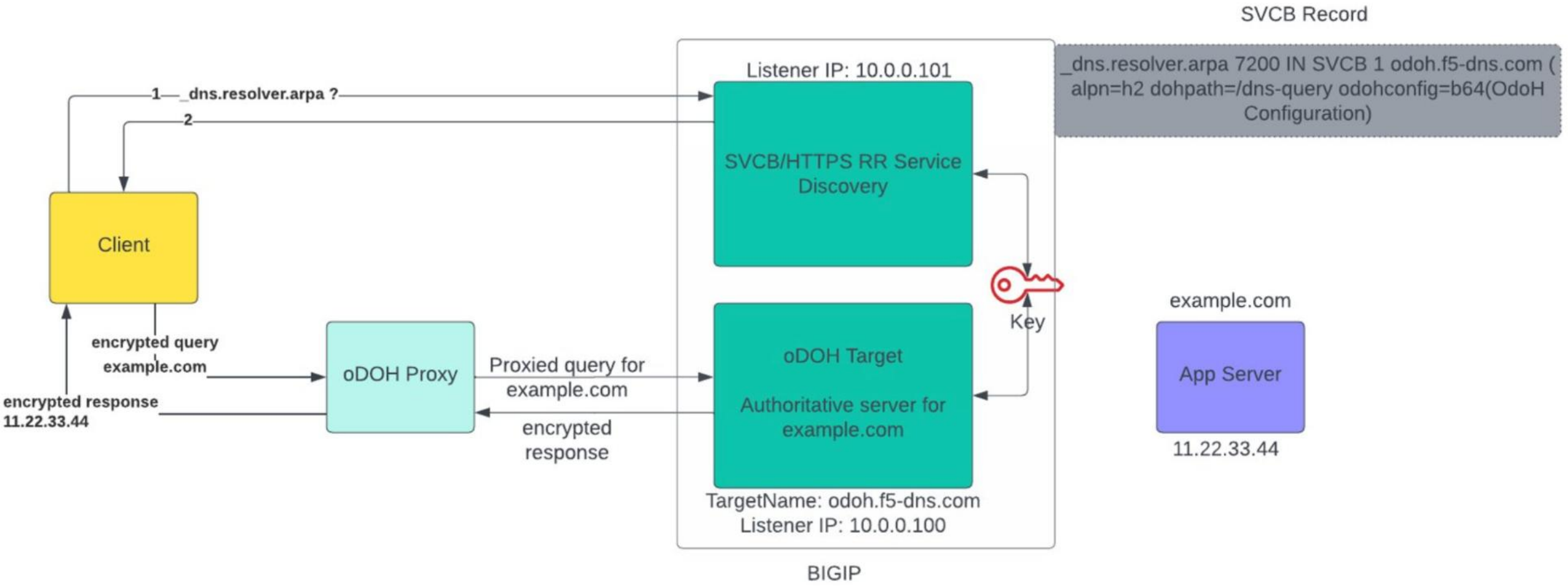
ODoH Relay KHÔNG biết:
- Nội dung truy vấn DNS
- Nội dung phản hồi DNS
- Máy chủ DNS được truy vấn

DoH Server KHÔNG biết:
- Địa chỉ IP của Client
- Có Relay ở giữa
- Danh tính người dùng

KÝ HIỆU

Q : Truy vấn DNS
R : Phản hồi DNS
$E_{pkR}(x)$: Mã hóa x bằng khóa công khai của Relay
HPKE : Giao thức mã hóa (Hybrid Public Key Encryption)

ODoH trên nền tảng F5 BIG-IP



S/Gi Firewall tích hợp đa dịch vụ