Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

VPN su Hardware Open Source

Antonio Francesco Gentile, *Davide Macrì, Emilio Greco*

RT- ICAR-CS-23-04 **Maggio 2023**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR)
– Sede di Cosenza, Via P. Bucci 8-9C, 87036 Rende, Italy, URL: *www.icar.cnr.it*
– Sezione di Napoli, Via P. Castellino 111, 80131 Napoli, URL: *www.icar.cnr.it*
– Sezione di Palermo, Via Ugo La Malfa, 153, 90146 Palermo, URL: *www.icar.cnr.it*

Indice generale

Introduzione

In questo lavoro si analizzano diverse soluzioni tecnologiche per realizzare una rete privata virtuale (VPN) e poter così garantire una comunicazione privata e confidenziale sulla rete Internet. La VPN ad oggi è considerata una delle tecnologie più affidabili a questo scopo, poiché offre la possibilità di apportare correzioni ai protocolli e/o aggiornamenti immediati per colmare eventuali falle di sicurezza che si riscontrano nel tempo. Lo studio condotto analizza possibili soluzioni attraverso il firmware open source OpenWrt 21.x utilizzando differenti sistemi operativi lato server come Debian 11 x64 e Mikrotik 7.x, entrambi virtualizzati, insieme a diversi tipi di client come Windows 10/11, iOS 15, Android 11, OpenWrt 21.x, Debian 11 x64 e Mikrotik 7.x.

L'obiettivo del lavoro è fare una disamina degli algoritmi VPN più comunemente utilizzati, concentrandoci sulle implementazioni più recenti di hardware e software che rendono la connettività sicura anche in luoghi esterni con scarsa connettività di rete.

Il primo obiettivo è quello di individuare gli algoritmi in grado di garantire un'elevata efficienza nella trasmissione e nella crittografia dei dati. Il secondo obiettivo è quello di identificare gli algoritmi VPN che offrono la massima compatibilità con le infrastrutture tecnologiche esistenti, in modo da ottenere un sistema di connessione sicuro per reti IoT geograficamente sparse in aree difficili da gestire come zone suburbane o rurali. Il terzo obiettivo è quello di utilizzare firmware open su router con prestazioni limitate, in modo da assicurarci di garantire al contempo la compatibilità con diversi protocolli VPN.

VPN – Virtual Private Network

Le moderne infrastrutture IT possono coprire vaste aree geografiche e, di conseguenza, richiedono infrastrutture tecnologiche sicure, affidabili e che nel contempo garantiscano costi ridotti, sia in termini di hardware che di tempo di gestione.

La rete privata virtuale (VPN) rappresenta una delle tecnologie più affidabili per soddisfare questo tipo di esigenza, passando attraverso le architetture "vecchie" (PSTN) alle più moderne reti 4G/5G.

Le VPN creano una connessione sicura tra il client dell'utente e il punto di accesso remoto. Il traffico viene crittografato per proteggerlo da eventuali intercettazioni. Tutto ciò avviene attraverso i server VPN, ai quali il traffico Internet dell'utente viene instradato prima di raggiungere la sua destinazione. Ciò consente di utilizzare le connessioni Wi-Fi pubbliche in modo più sicuro.

Queste connessioni possono essere facilmente intercettate, ma grazie a una VPN è possibile evitare intrusioni indesiderate durante la connessione da hotel, centri commerciali o mentre si è in attesa

all’aeroporto per il prossimo volo, soprattutto quando si accede a servizi sensibili come il proprio home banking. In questi casi, è l'effetto della crittografia offerto dalla VPN a fare la differenza. Viene creato un tunnel tra il client VPN e il server sulla rete pubblica per proteggere la connessione e garantire sicurezza e privacy agli utenti. La connessione viene iniziata dal client che comunica con il server e, una volta stabilita la connessione, viene creato il tunnel e i messaggi vengono crittografati tra le due parti autenticate del collegamento VPN.

Sono stati proposti molti tipi di protocolli VPN che offrono diversi livelli di sicurezza e funzionalità. Presentano quindi anche prestazioni diverse in termini di latenza e throughput. La scelta della soluzione VPN corretta è fondamentale per le prestazioni del sistema. Inoltre, l'interoperabilità con l'hardware è importante per l'esperienza che ha l’utente su dispositivi oggi in commercio.

Allo stato dell’arte possiamo distinguere le VPN raggruppandole per il tipo di protocollo utilizzato: IPsec o SSL.

Nel nostro lavoro, abbiamo considerato le seguenti tipologie di protocollo IPsec:

• IKEv1-XAUTH, IKEv1-L2TP, IKEv1 RSA

• IKEv2 RSA

• IKEv1 SITE TO SITE PSK, SITE TO SITE RSASIG

• IKEv2 SITE TO SITE RSASIG, IKEv2 SITE TO SITE PSK

• IKEv2 XFRMI ROUTE BASED

E le seguenti VPN basate su SSL:

• OpenVPN: ROAD WARRIORS, SITE TO SITE, SITE TO MULTI SITE

• Accel-ppp: SSTP ROAD WARRIORS, SSTP SITE TO SITE, SSTP SITE TO MULTI SITE

• Wireguard: SITE TO SITE, SITE TO MULTI-SITE, ROAD WARRIORS

• Ocserv: SITE TO SITE, ROAD WARRIORS

L'obiettivo principale che si siamo preposti è stato costruire un'infrastruttura Open Source per dispositivi intelligenti in ambiente IoT, da utilizzare in ambienti esterni con scarsa connettività di rete.

Il firmware OpenWRT consente di gestire connessioni VPN IPsec (Xauth, L2TP, X509 IKEV1 e IKEV2), client/server VPN per OpenVPN, OpenConnect (conosciuto anche come Cisco AnyConnect), SSTP (Microsoft ha sostituito il vecchio e ormai insicuro PPTP) e Wireguard. Consente inoltre l'utilizzo di sistemi di gestione del routing dinamico attraverso software come Quagga, Babeld

e FRR, consentendo al sistema di creare reti mesh realizzate tramite VPN punto-punto e punto-multipunto. Una volta creata l'infrastruttura, è possibile installare il software Mosquitto per gestire la parte IoT. Mosquitto è un servizio molto leggero che può essere configurato sia come client che come broker, offrendo funzionalità di concentrazione generale disponibili su un singolo dispositivo.

Possibili architetture di una VPN

IPsec

IPsec viene utilizzato per gestire tunnel VPN crittografati a livello di Layer 3 dell'architettura OSI. È stato proposto come standard dall'IETF, l'organizzazione responsabile dello sviluppo tecnico di Internet.

IPsec offre tre principali funzioni:

1. Protocolli di trasferimento: Encapsulating Security Payload (ESP) e Authentication Header (AH).
2. Gestione del processo di crittografia: Internet Key Exchange (IKE) e Internet Security Association and Key Management Protocol (ISAKMP).
3. Database: Security Policy Database (SPD) e Security Association Database (SAD).

Attraverso i protocolli AH e ESP, IPsec garantisce l'integrità e l'autenticità dei dati trasmessi. Il protocollo AH, tramite l'estensione Packet Accelerator, autentica la fonte dei dati e protegge contro la modifica dei pacchetti durante la trasmissione. Aggiunge anche un numero di sequenza nell'intestazione per prevenire l'invio di pacchetti duplicati.

Il protocollo ESP, oltre alla verifica dell'identità e dell'integrità dei dati, fornisce anche la crittografia dei dati in sospeso. Tuttavia, va notato che l'autenticazione ESP non considera l'intestazione IP esterna, quindi non è completa. Pertanto, è necessaria un ulteriore incapsulamento per consentire una corretta consegna dei contenuti ESP, specialmente quando si attraversano reti collegate tramite Network Address Translation (NAT), com'è comune nelle reti private xDSL.

IPsec può essere configurato per funzionare in due modalità: Tunnel e Transport. Nella modalità "transport", il protocollo di trasferimento viene aggiunto tra l'intestazione del pacchetto IP, che rimane invariata, e l'area dei dati. La protezione inizia sul computer mittente e si estende fino al computer di destinazione. Una volta ricevuto il pacchetto, i dati originali vengono decompressi e resi disponibili. Questa modalità offre un tempo di elaborazione molto ridotto, garantendo la sicurezza dei dati solo per quanto riguarda gli indirizzi di origine e destinazione. È adatta per le connessioni "Host 2 Host" o "Host 2 Router".

Nella modalità "tunnel", i pacchetti dati ricevono un nuovo header IP completo, nascondendo l'indirizzo originale, l'indirizzo di destinazione e i dati. Viene inoltre generato un nuovo header per il

protocollo di trasferimento, creando una modalità "incapsulata". La modalità "tunnel" viene utilizzata per le connessioni "Site 2 Site", "Host 2 Site" e "Host 2 Host".

SSL/TLS Based VPN

La VPN SSL/TLS (Virtual Private Network basata su Secure Sockets Layer) offre una soluzione VPN standard che si basa su un browser web nel livello di trasporto o viene sviluppata utilizzando applicazioni client/server specifiche. I socket vengono utilizzati per il trasferimento dei dati tra mittente e destinatario. Esistono due tipi generali di implementazione per la VPN SSL/TLS.

SSL/TLS Portal VPN - SSL/TLS Portal VPN: In questo scenario, l'accesso ai servizi sicuri viene ottenuto tramite una singola connessione SSL/TLS standard al server web di destinazione. Il client può accedere al gateway della VPN SSL/TLS tramite un normale browser web, fornendo i parametri necessari per negoziare l'autenticazione.

SSL/TLS Tunnel VPN: In questo scenario, il client VPN può accedere a più servizi/host di rete (come nel caso di OpenVPN, OpenConnect e SSTP). Nella comunicazione SSL/TLS classica, vengono utilizzate due chiavi per crittografare i dati: una chiave pubblica condivisa tra tutti e una chiave privata specifica per ogni punto finale. Per aumentare ulteriormente il livello di sicurezza, è possibile utilizzare l'autenticazione a due fattori, come l'OTP (One-Time Password) o altri metodi. Nella comunicazione IPsec, una volta che il client viene autenticato presso la VPN, ha accesso completo alla rete privata, mentre nella VPN SSL/TLS è possibile controllare l'accesso in modo più dettagliato, consentendo la creazione di tunnel specifici per le applicazioni tramite socket anziché per l'intera rete. È anche possibile creare "ruoli di accesso" specifici (profilo di accesso con diritti specifici per utenti diversi).

Linux Daemons

Una VPN basata su IPsec su sistemi Linux prevede l'implementazione tramite software dei protocolli IKE, AH ed ESP, utilizzando i moduli appropriati resi disponibili dallo stesso kernel.

Il protocollo IKE (Internet Key Exchange) ha lo scopo di autenticare i peer della VPN (utilizzando una chiave precondivisa, l'inserimento di una chiave pubblica o freeradius), generare dinamicamente le chiavi e condividerle con i peer della VPN. Le chiavi vengono utilizzate anche per la seconda fase di IPsec proveniente da IKE. Nell'implementazione, Libreswan utilizza il programma bar del progetto per implementare il protocollo IKE.

Il protocollo ESP (Encapsulating Security Payload) rappresenta la specifica effettiva delle politiche concordate tra i partecipanti, ed è implementato nello stack IPsec del kernel Linux (NETEY/XFRM).

Libreswan/Strongswan

LibreSwan e StrongSwan sono implementazioni open source del protocollo IPsec, basate su OpenSwan e sul progetto FreeSwan. Sono disponibili come pacchetti pronti all'uso nelle distribuzioni Linux come RedHat. Istruzioni dettagliate sono fornite nel codice del progetto per la compilazione su piattaforme Linux. Dopo il processo di installazione e una corretta configurazione, si otterrà un gateway VPN IPsec in grado di proteggere i dati in transito tra i vari membri della rete.

I file di configurazione di Libreswan non sono compatibili con quelli di StrongSwan, anche se il formato di ipsec.conf è identico. Diverse opzioni hanno significati diversi, altre sono mutualmente assenti a causa delle architetture supportate. Ad esempio, in Libreswan non è possibile abilitare il supporto L2TP IPsec di Android, poiché è fissato nel client con la versione DH2 ed è disabilitato nella fase di compilazione. StrongSwan e Libreswan supportano entrambi VPN basate su politiche (Policy-Based) e basate su route (Route-Based), ma nel primo caso possono essere utilizzate in modo mutuamente esclusivo a meno che non si passi dalla configurazione "classica" (ipsec.conf) alla nuova (swanctl.conf), mentre nel secondo caso sono supportate entrambe le politiche di default attraverso appositi flag.

Accel-PPP

Accel-PPP è un concentratore VPN progettato per garantire elevate prestazioni sui sistemi Linux e consente all'utente di gestire tecnologie VPN standard con un'applicazione singola. Molti progetti open source forniscono servizi VPN, ma si specializzano in una specifica tecnologia. Con Accel-PPTP, si dispone di un sistema tutto in uno con configurazione, gestione e monitoraggio centralizzati. Accel-PPP consente di gestire i protocolli: PPTP, PPPoE, L2TPv2, SSTP e IPoE. La registrazione dei dati può essere configurata tramite file o l'uso dei servizi Radius. L'autenticazione è gestita attraverso i meccanismi: PAP, CHAP (md5), MSCHAP-v1 e MSCHAP-v2, mentre EAP non è supportato. Tutti i tunnel PPPoE, PPTP e L2TP utilizzano appositi moduli del kernel per ottimizzare le prestazioni.

Operative Systems and Hardware Platforms

Nel panorama attuale, sono disponibili numerosi sistemi operativi e piattaforme HW/SW dedicate alle reti e alle comunicazioni sicure. Tra questi abbiamo: MikroTik che sviluppa MikroTik RouterOS, il sistema operativo delle schede RouterBOARD; OpenWrt, sviluppato dal progetto OpenWrt, un sistema operativo Linux integrato utilizzato su dispositivi embedded per il routing del traffico di rete; PfSense, basato su FreeBSD, un router e firewall open source con funzionalità che permettono di gestire minacce unificate, multiWAN e bilanciamento del carico; OPNsense, un altro firewall open source basato su FreeBSD che garantisce alta sicurezza, prevenzione delle intrusioni, shaping del

traffico e servizi di Captive Portal; IPFire, basato su Linux, una distribuzione progettata per utilizzare la macchina come firewall interno o perimetrale; VyOS, basato su Linux open source e distribuito dall'azienda Sentrium. È open source e progettato per proteggere la rete e i dati aziendali con elevate prestazioni; Gargoyle, un firmware progettato per utilizzare la macchina come firewall interno o perimetrale; LibreMesh, un software open source per reti comunitarie Mesh senza complicazioni tecniche. In questo articolo, ci concentreremo sul firmware OpenWrt e sulla piattaforma MikroTik per effettuare un confronto.

OpenWRT

OpenWrt è una distribuzione originariamente pensata per l'uso su router wireless, per estendere le loro funzionalità rispetto al firmware fornito dal produttore. Il sistema operativo garantisce un filesystem con permessi di scrittura per l'utente, consentendo, tra le altre cose, l'installazione di software di terze parti e quindi la possibilità di ampliare le sue funzionalità. Ciò permette di utilizzare il software di routing più recente e garantisce maggiore sicurezza e meno bug rispetto al software preinstallato fornito dal produttore, specialmente su dispositivi più vecchi non più supportati.

Può essere installato anche su hardware personalizzato, come specifiche schede, e nel caso delle piattaforme x86-64 supporta anche la virtualizzazione, consentendo la creazione di reti di container per servizi ad hoc, oltre a fornire accesso di rete a tutti i dispositivi nella LAN.

MikroTik

MikroTik è un'azienda che produce attrezzature per reti e connettività Internet, in particolare router e apparecchiature per connessioni wireless a banda larga per Internet Service Provider wireless. È presente in quasi tutti i paesi del mondo. L'esperienza di MikroTik nella creazione di hardware e sistemi di routing altamente compatibili con gli standard del settore, ha portato alla creazione nel 1997 del software RouterOS, con un elevato controllo e flessibilità per tutti i tipi di router e interfacce, sviluppato sul kernel Linux. Grazie a RouterOS, qualsiasi PC o scheda MikroTik RouterBOARD può diventare un router dedicato. Essendo dispositivi proprietari, la flessibilità nell'installazione di pacchetti per funzionalità aggiuntive, sebbene rispettabile (supporta IoT, Lora e 4G/5G), è inferiore a quella di OpenWrt.

Descrizione di diverse soluzioni VPN implementate

Per creare una VPN ci sono diverse soluzionisia HW che SW, ad esempio attraverso l’uso Mikrotik RouterBoards, o implementando uno stack software appropriato sul proprio server, attraverso ad esempio le feature messe a disposizione dal sistema operativo Debian che consente di definire

particolari proprietà alla rete VPN a seconda dell'implementazione scelta. In particolare, ci concentreremo su tre macro scenari applicativi:

- Site to Site scenario: dove due uffici remoti sono connessi in modo sicuro. Figura 1
- Site to Multi-Site scenario: dove più uffici remoti possono essere messi in comunicazione tra loro attraverso una connessione sicura, Figura 2
- Road Warriors scenario: in cui più utenti di uffici remoti comunicano in modo sicuro con un particolare ufficio locale, mostrato in Figura 3.

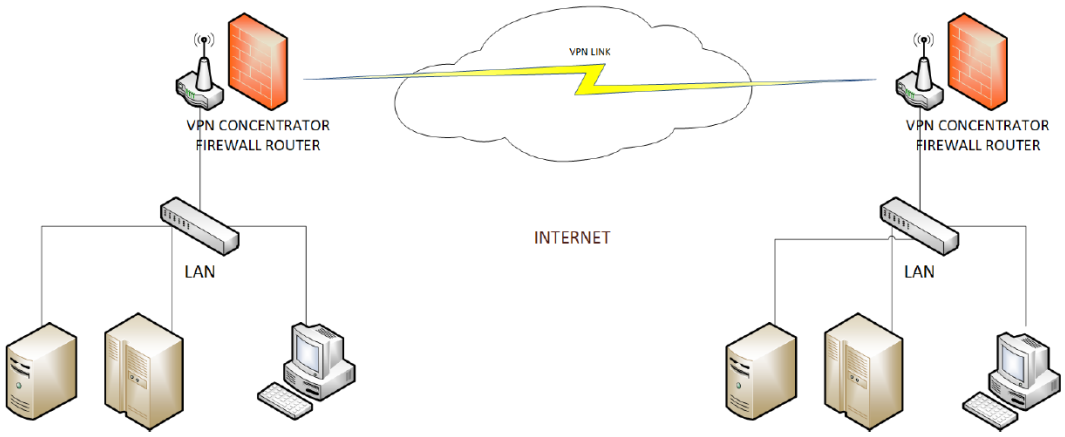

Figura 1 - Site to Site scenario

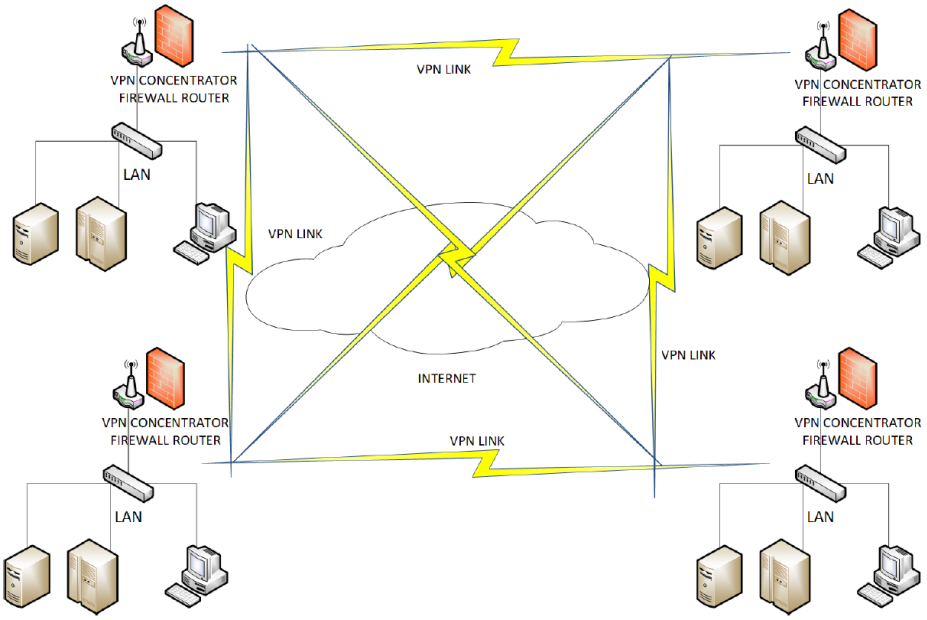

Figura 2 - Site to MultiSite scenario

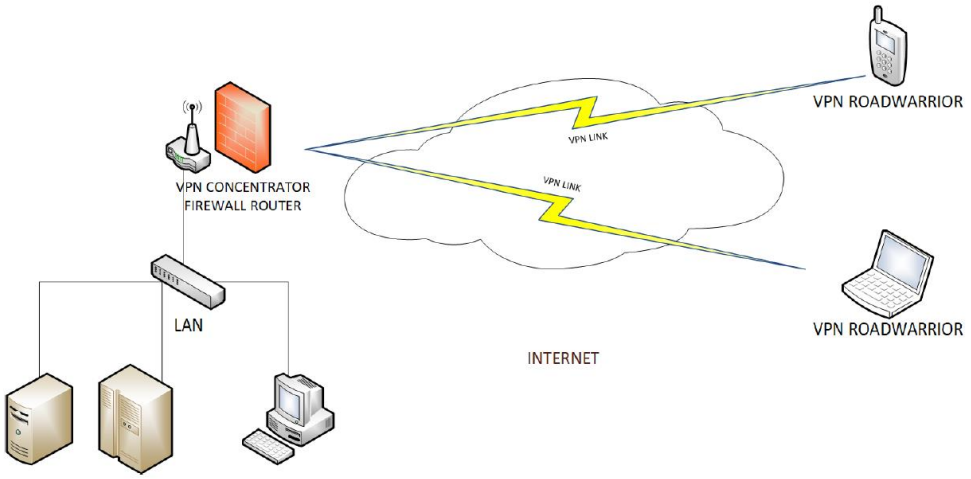

Figura 3 - Road Warriors scenario

Queste soluzioni forniscono crittografia e integrità dei dati in transito basandosi su algoritmi di crittografia che vanno da Blowfish ad AES fino alle implementazioni che utilizzare curve ellittiche. A seconda del tipo di dispositivo/rete da interconnettere, sono disponibili varie alternative, soprattutto nel caso di Road Warriors (RW), passando dall'autenticazione tramite PSK + XAUTH (es. in IPsec) a quella tramite certificati, oppure a soluzioni in due passaggi: tramite one-time password (OTP) o credenziale integrativa (nel caso di RADIUS + VPN IPsec/OpenVPN/OpenConnect).
L'aumento esponenziale di tecnologie come l'IoT, ed il conseguente sviluppo di paradigmi comunicativi come il “Fog Computing” o “Approcci orientati al cloud” (ad es. AMAZON AWS) o cluster multisito (ad es. realizzati tramite Kubernetes) e l’aumento di offerta di tecnologie portanti come fibra/PSTN o portanti 4G/5G, ha generato e genererà anche in futuro un sempre crescente volume di dati, i quali, anche in ottemperanza al recente “General data protection regolamento” (GDPR), devono essere gestiti e protetti correttamente.

Un grande vantaggio derivante dall'uso di OpenWRT quale sistema operativo delle apparecchiature di rete, è quello di consentire l'implementazione di diverse tecnologie di VPN su tutti i modelli di router e dispositivi compatibili. L'ampia gamma di "bridges" supportati permette, soprattutto nel caso di reti IoT, di interfacciarsi con protocolli di terze parti, e di utilizzare gateway perimetrali, che fanno uso di LoRa o Zigbee, oltre a quelli che supportato lo stack classico TCP/IP.
Se altresì considerare che anche la versione x86-64 di OpenWRT supporta facilmente la virtualizzazione, permettendo la creazione di reti Fog di microservizi e IoT multiprotocollo in tempi

trascurabili. Un esempio potrebbe essere dato dall'installazione di reti di sensori outdoor su aree coperte in WAN da reti 4G/5G e localmente configurabile ed elaborabile con un approccio “Edge Computing”.