
RA3. Implantació de tècniques segures d'accés remot a un sistema informàtic

Índex

1. Escenaris amb connexió a xarxes públiques	1
2. Seguretat perimètrica	2
2.1 Elements bàsics	2
2.2 Zones de risc: DMZ	2
2.3 Arquitectura feble de subxarxa protegida (screened subnet feble)	2
2.4 Arquitectura forta de subxarxa protegida (screened subnet forta)	3
3. Protocols segurs de comunicació	3
4. Xarxes privades virtuals (VPN)	4
4.1 Concepte i tipus	4
4.2 Beneficis i inconvenients enfront de línies dedicades	4
4.3 Tècniques de xifratge: clau pública i clau privada	4
4.4 VPN a escala de xarxa: IPSec	5
4.5 VPN a nivell d'aplicació: SSH	5
5. Implantació d'una passarel·la d'accés remot	6
5.1 Escenari	6
5.2 Instal·lació i configuració del servidor	6
5.3 Configuració del client	7
5.4 Regles al tallafocs de la passarel·la	7
6. Mètodes d'autenticació d'usuaris remots	8
7. Servidor remot d'autenticació: integració amb RADIUS	8
7.1 Per què centralitzar	8
7.2 Instal·lació de FreeRADIUS	9
7.3 Integració de la passarel·la amb RADIUS	9

Cicle formatiu: Administració de sistemes informàtics en xarxa (ASIX)

Mòdul: 0378. Seguretat i alta disponibilitat

NOTA

Per als exemples pràctics utilitzarem una topologia de laboratori amb tres màquines: un **router/firewall** amb dues o tres interfícies de xarxa (WAN, LAN, DMZ), un **servidor intern** (LAN) i un **client remot** que simula un usuari des d'Internet.

1. Escenaris amb connexió a xarxes públiques

Quan un sistema informàtic deixa de ser una illa i es connecta a Internet, apareixen riscos que no existeixen en una xarxa tancada. Els escenaris típics que obliguen a fortificar la xarxa són:

- **Accés de treballadors en mobilitat o teletreball:** cal que un usuari es connecti als recursos interns (fitxers, ERP, bases de dades) des de fora de l'oficina, sovint des de xarxes no confiables (wifis públiques, xarxes domèstiques).
- **Interconnexió de seus:** una empresa amb diverses seus necessita que les seves xarxes locals es comuniquin com si fossin una de sola.
- **Publicació de serveis:** un servidor web, de correu o de VPN ha de ser accessible des d'Internet, però la resta de la infraestructura (bases de dades, directori actiu) no ha d'estar exposada.
- **Administració remota de sistemes:** els administradors necessiten gestionar servidors i equips de xarxa sense haver de desplaçar-se físicament.
- **Accés de tercers:** proveïdors o clients que necessiten accedir a un recurs concret, sense donar-los accés a tota la xarxa interna.

En tots aquests casos, el principi que guia el disseny és el mateix: **exposar el mínim imprescindible i segmentar la resta**. D'aquí neix la seguretat perimètrica.

2. Seguretat perimètrica

2.1 Elements bàsics

El perímetre de xarxa és la frontera entre allò que controlem (la xarxa interna) i allò que no controlem (Internet). Els elements bàsics que en formen part són:

Element	Funció
Router frontera	Connecta la xarxa interna amb l'exterior; sol fer NAT.
Tallafocs (firewall)	Filtra el trànsit segons regles (IP, port, protocol, estat de la connexió).
IDS/IPS	Detecta (IDS) o detecta i bloqueja (IPS) patrons de trànsit maliciós.
Proxy	Intermedia connexions (sortints o entrants), pot fer cache i filtrat de contingut.
Passarel·la VPN	Punt d'entrada xifrat per a usuaris o xarxes remotes.
Bastion host	Servidor endurit (hardened) exposat a Internet, únic punt d'entrada a la DMZ.

2.2 Zones de risc: DMZ

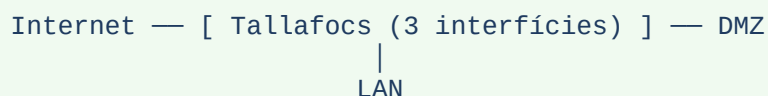
Segons el nivell d'exposició i confiança, classifiquem la xarxa en zones:

- **Xarxa externa (Internet)**: zona no confiable, fora del nostre control.
- **DMZ (zona desmilitaritzada)**: xarxa intermèdia on es col·loquen els serveis que han de ser accessibles des d'Internet (web, correu, DNS públic, passarel·la VPN). Si un d'aquests serveis és compromès, l'atacant no arriba directament a la LAN.
- **Xarxa interna (LAN)**: zona de màxima confiança, on hi ha els recursos crítics (directori actiu, bases de dades, fitxers). Mai s'hi accedeix directament des d'Internet.

La regla d'or de la DMZ és: **el trànsit d'Internet pot arribar a la DMZ; el trànsit de la DMZ cap a la LAN és molt restringit; el trànsit d'Internet mai arriba directament a la LAN.**

2.3 Arquitectura feble de subxarxa protegida (screened subnet feble)

Utilitza un únic tallafocs amb tres interfícies (WAN, DMZ, LAN):



Avantatges: senzilla, econòmica, un sol punt de gestió.

Inconvenients: un únic punt de fallada. Si el tallafocs és compromès o mal configurat, tota la protecció cau alhora. Un error de regles pot exposar la LAN directament.

2.4 Arquitectura forta de subxarxa protegida (screened subnet forta)

Utilitza **dos tallafocs** (idealment de fabricants diferents), amb la DMZ situada entre tots dos:

Internet — [Tallafocs extern] — DMZ — [Tallafocs intern] — LAN

- El **tallafocs extern** filtra el trànsit d'Internet cap a la DMZ (obre només els ports dels serveis publicats).
- El **tallafocs intern** filtra el trànsit de la DMZ cap a la LAN (molt més restrictiu; idealment només permet connexions concretes iniciades des de la LAN o respostes a aquestes).

Avantatges: defensa en profunditat. Un atacant que compromet un servidor de la DMZ encara ha de superar un segon tallafocs, possiblement d'un fabricant diferent (evita que una mateixa vulnerabilitat afecti els dos).

Inconvenients: més cost, més complexitat de gestió i manteniment.

3. Protocols segurs de comunicació

Abans de parlar de VPN cal saber quins protocols proporcionen xifratge i autenticació, i a quin nivell de la pila OSI/TCP-IP actuen:

Protocol	Nivell	Àmbit d'ús típic
IPSec	Xarxa (nivell 3)	VPN site-to-site, VPN d'accés remot a escala de xarxa
SSL/TLS	Transport/sessió (nivell 4-5)	HTTPS, VPN SSL (portal web o client), correu segur (IMAPS, SMTPS)
SSH	Aplicació (nivell 7)	Administració remota, túnels d'aplicació, SFTP
WireGuard	Xarxa (nivell 3, en espai d'usuari/kernel)	VPN moderna, alternativa lleugera a IPSec
RADIUS/TACACS+	Aplicació	Autenticació i autorització centralitzada d'accessos

La diferència pràctica és **què queda protegit**: IPSec xifra tot el trànsit IP entre dos punts (transparent a les aplicacions), SSL/TLS xifra una connexió concreta pel que fa a la sessió, i SSH xifra una sessió o un túnel concret a nivell d'aplicació.

4. Xarxes privades virtuals (VPN)

4.1 Concepte i tipus

Una **VPN** crea un canal de comunicació xifrat i autenticat sobre una xarxa no confiable (normalment Internet), simulant que els extrems estan connectats per una xarxa privada.

Tipus segons l'ús:

- **Site-to-site**: connecta dues xarxes senceres (per exemple, dues seus d'una empresa). El túnel es crea entre dos routers/passarel·les.
- **Accés remot (client-to-site)**: connecta un únic dispositiu (portàtil, mòbil) a la xarxa interna a través d'una passarel·la. És el cas d'aquest RA.

4.2 Beneficis i inconvenients enfront de línies dedicades

	Línia dedicada	VPN sobre Internet
Cost	Alt (lloguer de circuit)	Baix (només connexió a Internet)
Latència/QoS	Garantida pel proveïdor	Depèn d'Internet, sense garanties
Desplegament	Lent (instal·lació física)	Ràpid (configuració de programari)
Escalabilitat	Costosa d'ampliar	Molt escalable (nous usuaris = nova configuració)
Seguretat	Física (el mitjà no és compartit)	Criptogràfica (depèn de la implementació)

4.3 Tècniques de xifratge: clau pública i clau privada

Les VPN modernes es basen en **criptografia asimètrica** per a l'intercanvi inicial de claus i **criptografia simètrica** per xifrar el volum de dades (és molt més ràpida):

1. Cada extrem té un parell de claus: una **clau pública** (es pot compartir) i una **clau privada** (secreta, mai surt del dispositiu).
2. Durant l'establiment del túnel (per exemple, amb un intercanvi Diffie-Hellman autenticat amb les claus públiques), els dos extrems acorden una **clau de sessió simètrica** compartida.
3. Tot el trànsit de dades es xifra amb aquesta clau simètrica (AES, ChaCha20...), molt més eficient que xifrar cada paquet amb RSA.

Aquest esquema és el que trobem tant a IPsec (IKE) com a TLS (handshake) com a SSH i WireGuard.

4.4 VPN a escala de xarxa: IPSec

IPSec no és un sol protocol sinó un conjunt:

- **AH (Authentication Header)**: garanteix integritat i autenticitat, però **no xifra** les dades.
- **ESP (Encapsulating Security Payload)**: xifra i autentica les dades. És el que s'utilitza gairebé sempre en la pràctica.
- **IKE (Internet Key Exchange)**: protocol per negociar i intercanviar les claus de forma segura abans d'establir el túnel.

Modes de funcionament:

- **Mode transport**: xifra només les dades del paquet IP (payload), mantenint la capçalera original. S'utilitza entre dos hosts finals.
- **Mode túnel**: encapsula tot el paquet IP original (capçalera inclosa) dins d'un de nou. És el mode habitual per a VPN entre passarel·les, ja que amaga la xarxa interna original.

CONSELL

A la pràctica, la solució IPSec més estesa en entorns Linux és **strongSwan**, i és compatible amb clients nadius de Windows, macOS, iOS i Android (IKEv2), fet que la fa molt útil per a VPN d'accés remot sense instal·lar programari addicional al client.

4.5 VPN a nivell d'aplicació: SSH

SSH permet crear túnels xifrats per a aplicacions concretes sense muntar una VPN completa:

```
# Túnel local: accedim a un servei intern (ex: escriptori remot al
↪ port 3389)
# a través del servidor SSH bastion, com si fos local al nostre equip
↪ (port 13389)
ssh -L 13389:servidor-intern:3389 usuari@bastion.exemple.cat

# Túnel remot: exposem un servei nostre cap a la xarxa remota
ssh -R 8080:localhost:80 usuari@servidor-remot.exemple.cat

# SSH com a proxy SOCKS: tot el trànsit d'una aplicació passa xifrat
↪ pel túnel
ssh -D 1080 usuari@bastion.exemple.cat
```

Diferència clau amb una VPN real: SSH tunneling xifra connexions concretes (aplicació per aplicació), mentre que IPSec o WireGuard xifren **tot** el trànsit IP entre els dos extrems, de manera transparent per a qualsevol aplicació.

5. Implantació d'una passarel·la d'accés remot

Muntarem una passarel·la VPN amb **WireGuard**, per la seva senzillesa de configuració i el seu ús creixent en entorns de producció, com a exemple pràctic de VPN a escala de xarxa amb clau pública/privada.

5.1 Escenari

- **Passarel·la** (a la DMZ o al tallafocs frontera): interfície pública 203.0.113.10, interfície WireGuard 10.10.0.1/24.
- **Client remot**: obtindrà una IP virtual 10.10.0.2/24 i, a través del túnel, accedirà a la LAN interna 192.168.10.0/24.

5.2 Instal·lació i configuració del servidor

```
sudo apt update
sudo apt install wireguard -y

# Generem el parell de claus del servidor
wg genkey | sudo tee /etc/wireguard/server_private.key
sudo cat /etc/wireguard/server_private.key | wg pubkey | sudo tee
↪ /etc/wireguard/server_public.key
```

Fitxer /etc/wireguard/wg0.conf al servidor:

```
[Interface]
Address = 10.10.0.1/24
ListenPort = 51820
PrivateKey = <clau_privada_servidor>
# Reenviem trànsit del túnel cap a la LAN interna i apliquem NAT si cal
PostUp = iptables -A FORWARD -i wg0 -o eth1 -j ACCEPT
PostUp = iptables -A FORWARD -i eth1 -o wg0 -j ACCEPT
PostDown = iptables -D FORWARD -i wg0 -o eth1 -j ACCEPT
PostDown = iptables -D FORWARD -i eth1 -o wg0 -j ACCEPT

[Peer]
# Client remot
PublicKey = <clau_publica_client>
AllowedIPs = 10.10.0.2/32
```

Cal habilitar l'encaminament IP al sistema:

```
echo 'net.ipv4.ip_forward = 1' | sudo tee -a /etc/sysctl.conf
sudo sysctl -p
```

Aixequem la interfície i l'activem a l'arrencada:

```
sudo systemctl enable --now wg-quick@wg0
```

5.3 Configuració del client

```
wg genkey | tee client_private.key | wg pubkey > client_public.key
```

Fitxer wg0.conf al client:

```
[Interface]
Address = 10.10.0.2/24
PrivateKey = <clau_privada_client>

[Peer]
PublicKey = <clau_publica_servidor>
Endpoint = 203.0.113.10:51820
# Només enviem pel túnel el trànsit cap a la LAN interna (split tunnel)
AllowedIPs = 192.168.10.0/24, 10.10.0.0/24
PersistentKeepalive = 25
```

NOTA

Si a AllowedIPs del client hi poséssim 0.0.0.0/0, **tot** el trànsit d'Internet del client passaria pel túnel (full tunnel), útil per inspeccionar o filtrar la navegació dels usuaris remots, però consumeix més amplada de banda a la passarel·la.

5.4 Regles al tallafocs de la passarel·la

Cal obrir únicament el port UDP de WireGuard des d'Internet:

```
sudo iptables -A INPUT -p udp --dport 51820 -j ACCEPT
```

La resta de trànsit d'Internet cap a la passarel·la ha de quedar bloquejat: la passarel·la només ha d'exposar el servei VPN, seguint el mateix principi de mínima exposició de la seguretat perimètrica.

6. Mètodes d'autenticació d'usuaris remots

Un cop el túnel xifrat està establert, cal decidir **com s'autentica** l'usuari. No és el mateix xifrar el canal que verificar qui hi ha a l'altre extrem.

Mètode	Descripció	Seguretat
PAP (Password Authentication Protocol)	Envia usuari i contrasenya en clar (dins del túnel, però sense protecció addicional).	Baixa
CHAP (Challenge Handshake)	El servidor envia un repte (challenge); el client respon amb un hash de la contrasenya + el repte. La contrasenya mai viatja per la xarxa.	Mitjana
MS-CHAPv2	Variant de CHAP de Microsoft, amb autenticació mútua. Usat històricament amb PPTP/L2TP.	Mitjana
EAP (Extensible Authentication Protocol)	Marc extensible que permet diversos mètodes (EAP-TLS amb certificats, EAP-PEAP, EAP-MSCHAPv2...). Base de l'autenticació 802.1X i de molts servidors RADIUS.	Alta (segons el mètode EAP triat)
Certificats digitals (clau pública)	L'usuari es presenta amb un certificat signat per una CA de confiança, en lloc d'una contrasenya.	Alta
Autenticació multifactor (MFA)	Combina alguna cosa que l'usuari sap (contrasenya) amb alguna cosa que té (token, app OTP) o és (biometria).	Molt alta

A la pràctica, moltes passarel·les (IPSec amb IKEv2, VPN SSL) permeten combinar **certificat de màquina + usuari/contrasenya (o EAP)**, de manera que cal tant un dispositiu autoritzat com unes credencials vàlides.

7. Servidor remot d'autenticació: integració amb RADIUS

En lloc de mantenir una llista d'usuaris a cada passarel·la, el més habitual és **centralitzar l'autenticació** en un servidor dedicat. El protocol estàndard per a això és **RADIUS** (Remote Authentication Dial-In User Service).

7.1 Per què centralitzar

- Un sol lloc on donar d'alta, modificar o revocar usuaris.
- Es pot integrar amb el directori actiu o LDAP existent.
- Permet registrar (accounting) qui es connecta, quan i des d'on, útil per a auditoria.
- Diverses passarel·les (VPN, wifi corporativa, switches 802.1X) poden compartir el mateix servidor d'autenticació.

7.2 Instal·lació de FreeRADIUS

```
sudo apt update
sudo apt install freeradius -y
```

Donem d'alta un client RADIUS (la nostra passarel·la VPN) a `/etc/freeradius/3.0/clients.conf`:

```
client passarella-vpn {
    ipaddr      = 10.10.0.1
    secret      = SecretCompartit2024
    shortname    = vpn-gateway
}
```

Creem un usuari de prova a `/etc/freeradius/3.0/users`:

```
usuari1 Cleartext-Password := "Contrasenya123"
```

Reiniciem el servei i el provem en mode depuració:

```
sudo systemctl restart freeradius
sudo freeradius -X
```

Des d'una altra terminal, validem l'autenticació amb l'eina de proves inclosa:

```
radtest usuari1 Contrasenya123 localhost 0 SecretCompartit2024
```

Una resposta `Access-Accept` confirma que el servidor autentica correctament.

7.3 Integració de la passarel·la amb RADIUS

L'últim pas és configurar la passarel·la (per exemple, un servidor **strongSwan** amb mòdul EAP-RADIUS, o un OpenVPN amb el connector `radiusplugin`) perquè, en lloc de validar contrasenyes localment, delegui l'autenticació al servidor RADIUS.

Exemple de configuració a `/etc/strongswan.d/charon.conf` per activar l'agent EAP-RADIUS:

```
charon {
    plugins {
        eap-radius {
            servers {
                freeradius-server {
                    address = 192.168.10.5
                    secret = SecretCompartit2024
                    auth_port = 1812
                }
            }
        }
    }
}
```

```
}  
}
```

I a la configuració de la connexió IKEv2 (/etc/ipsec.conf), s'indica que l'autenticació de l'usuari es fa per EAP:

```
conn accesremot  
    left=%any  
    leftauth=pubkey  
    leftcert=serverCert.pem  
    right=%any  
    rightauth=eap-radius  
    rightsourc=10.10.0.0/24  
    auto=add
```

D'aquesta manera, el servidor s'autentica amb el client mitjançant certificat (l'usuari sap que es connecta a la passarel·la legítima), i l'usuari s'autentica mitjançant EAP contra el servidor RADIUS, que és qui finalment decideix si les credencials són vàlides.

Versions d'aquest document

- [HTML](#)
- [PDF](#)
- [ODT](#)
- [MD](#)

[Domini Públic \(CC0\)](#)