COMPITO SCRITTO in classe di SISTEMI E RETI su foglio protocollo sui seguenti argomenti:
NAT.
Firewall, definizioni.
Protezione: Dati, Risorse, Reputazione.
Sicurezza delle reti.
Host bastione, single e dual-homed.
Router e router filtranti.
Proxy server.

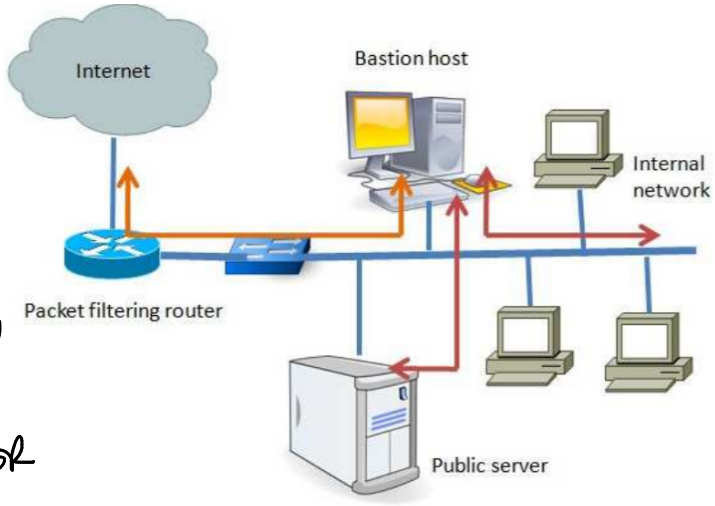
1 – Una ditta di materiali informatici possiede degli uffici collegati mediante una LAN interna. Uno o più server, collegati a internet, offrono dei servizi al pubblico.

Proponi delle architetture per la massima sicurezza basate su schemi di seguito elencati:

- Host bastion single homed **[2 punti]**
- Host bastion dual homed **[2 punti]**
- Bastion tra due router **[1 punto]**
- Avendo necessità di esporre all'esterno alcuni servizi, si decide la creazione di una terza zona in cui sia il traffico WAN che quello LAN siano fortemente limitati e controllati in modo da proteggere la LAN dai server collegati a internet. **[2 punti]**

Per ognuna delle soluzioni richieste illustra mediante schemi e spiega

a) la configurazione,
b) i collegamenti fisici,
c) i percorsi delle informazioni,
d) i pro e i contro.



BASTION HOST

PC SERVER

(PRIVATO) (PUBBLICO)

FILTRO DEL BASTION

Il bastion host si pone tra la connessione internet pubblica e la rete privata e filtra tutti i contenuti scambiati fra le due reti: in caso di attacco il sistema blocca l'attacco impedendo l'accesso alla rete locale. Questo computer ospita generalmente una singola applicazione, ad es. un proxy server, mentre tutti gli altri servizi non essenziali (come applicazioni, demoni ed utenti) vengono rimossi o limitati per ridurre al minimo la minaccia di infezione del sistema stesso

SINGLE-HOMED ⇒ ROUTER FILTRANTE + BASTION HOST (UNICA) [RISCHIO]

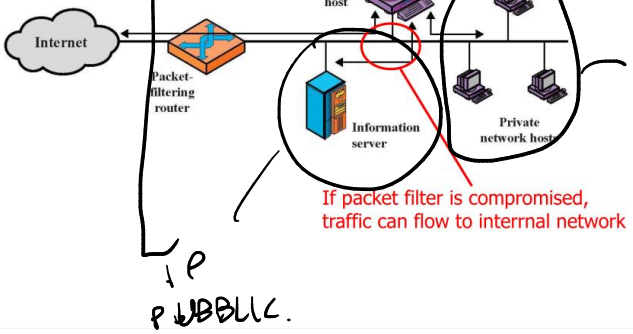
DUAL-HOMED ⇒ INTERFACCIA DI RETE + SEPARAZIONE

TIPI DI BASTION HOST

Un bastion host single homed, essendo dotato di un'unica interfaccia di rete, presenta un'architettura più semplice che riduce la superficie di attacco e il rischio di errori di configurazione che potrebbero compromettere la separazione tra reti. In un ambiente dual homed, sebbene si ottenga una separazione fisica delle interfacce, la maggiore complessità nella gestione (ad esempio nella configurazione del routing e delle regole firewall) può introdurre vulnerabilità qualora non vengano applicate rigorose misure di controllo. Pertanto, in linea di principio e con una corretta implementazione, il bastion host single homed è generalmente considerato più sicuro.

[Single-Homed Bastion Host] → 1 SOLO COLLEGAMENTO!

@ / (b)



DUT (80)

(W) 192.

PRIVATO = NAT

LAN

IP PUBBLICO ACCESSIBILE

Per ognuna delle soluzioni richieste illustra mediante schemi e spiega
a) la configurazione,
b) i collegamenti fisici, → ETHERNET (CAP. 7)
c) i percorsi delle informazioni,
d) i pro e i contro.

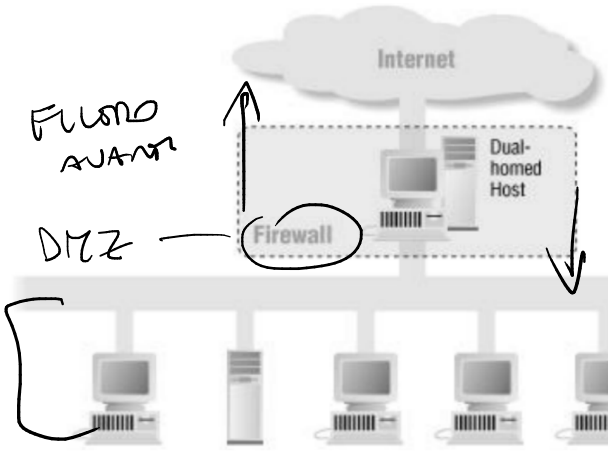
ROUTING DINAMICO (DHCP)

SINGLE-HOMED
- PRO → CONTROLLO PROCESSO FATTO DA TUTTI
- CONTRO → SI INTASA

```
[Internet/WAN] -- [Router] -- [Switch] -- [Bastion Host (1 NIC)]
                                \-- [Server DMZ]
                                \-- [LAN interna]
```

[DUAL-HOMED]

BASTION ⊂ DMZ, FIREWALL



FLUSSO AVANTI

FLUSSO INDIETRO

DMZ

Per ognuna delle soluzioni richieste illustra mediante schemi e spiega
a) la configurazione,
b) i collegamenti fisici, → ETHERNET (...)
c) i percorsi delle informazioni, → DHCP
d) i pro e i contro.

→ (W)LAN

```
          [Internet/WAN]
                |
          [Router WAN]
                |
          [Bastion Host]
          /           \
[Interfaccia 1]   [Interfaccia 2]
        |                 |
     [DMZ]          [LAN interna]
```

DUAL-HOMED

② INTERFACCE

- UNA VERSO INTERNET (→)
- UNA VERSO LA LAN (←)

PRO → MIGLIORE SEPARAZIONE

CONTRO → PIÙ COMPLESSA

[BASTION TRA DUE ROUTER] → FLUSSO CONNESSIONI (CISCO: REGOLA ROSSA!)

```
[Internet/WAN]
      |
  [Router WAN] → (1)
      |
      |---> [DMZ con server e/o bastion host] <---|
      |                                           |
  [Router LAN] → (2)                        [LAN interna]
```

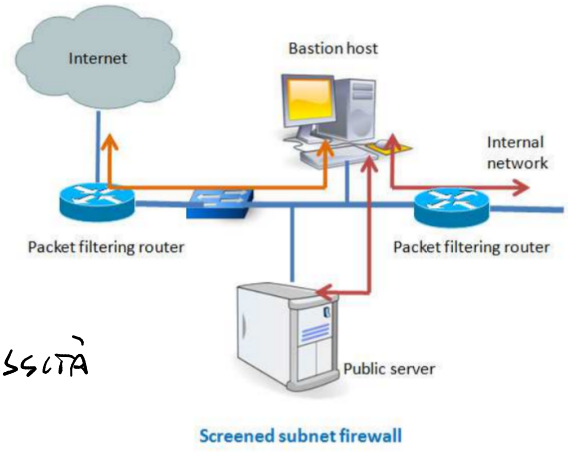
→ BASTION HOST

Per ognuna delle soluzioni richieste illustra mediante schemi e spiega
a) la configurazione,
b) i collegamenti fisici,
c) i percorsi delle informazioni,
d) i pro e i contro.

CONFIG. → DINAMICA
PERCORSI → CONTROLLATI (GRANULARE)

• **Bastion tra due router**

Questa è una delle configurazioni firewall più sicure. In questa configurazione, vengono utilizzati due router di filtraggio dei pacchetti e l'host del bastion è posizionato tra i due router. In un caso tipico, sia Internet che gli utenti interni hanno accesso alla sottorete schermata, ma il flusso di traffico tra le due sottoreti (uno è dall'host del bastione alla rete interna e l'altro è la sottorete tra i due router) è bloccato.



Screened subnet firewall

PRO: MOLTO SICURA

CONTRO → COMPLESSITÀ DI GESTIONE

Confronto sulla sicurezza

- **Host Bastion Single Homed**: più semplice ma meno sicuro perché la separazione tra LAN e DMZ è solo logica (VLAN, ACL) e poggia su un unico punto di falla (bastion host).
- **Host Bastion Dual Homed**: più sicuro del single homed perché separa fisicamente almeno due reti (WAN e DMZ/LAN), ma è più complesso da configurare.
- **Bastion tra due Router**: in genere considerata la soluzione più sicura e flessibile per creare una DMZ fisicamente isolata e proteggere la LAN; richiede però costi e competenze superiori.

2 – Elenca e spiega quali sono gli elementi da proteggere nei sistemi informatici. **[1 punto]**

SISTEMI → DATI! → CONFIDENZIALITÀ (DATI USATI)
→ INTEGRITÀ (NON PERSI)
→ DISPONIBILITÀ (PERSISTENTI)

RISCHI? → - FALSIFICAZIONI
- ATTACCHI DISTRIBUITI

3 – Spiega la sicurezza a livello di singola macchina e a livello di rete.
(Facoltativo se prescritto maggiore tempo) **[1 punto]**

SICUREZZA A LIV. MACCHINA (HOST)

→ AUDITING DEI LOG E REPORT (LOGGARE UN LIVELLO DEL TRAFFICO) AUMENTATO

SICUREZZA A LIV. RETE

→ FILTRAGGIO FIREWALL → HARDWARE, SOFTWARE REGOLE DISP. FILTRO TRAFFICO

→ DMZ (ZONA PROTETTA)

4 – La sicurezza a livello dei database contenuti nei server della ditta è ormai ben regolamentata, evidenzia le linee principali. Spiega poi, facendo anche degli esempi, le procedure da adottare nel caso di password, di dati personali, di dati sensibili. **[1 punto]**

PASSWORD
- DB PROTETTO
- CRIPTAZIONE PASSWORD
- METODOLOGIE AGGIUNTIVE DI SICUREZZA
- PIANI DI RECUPERO

FRAMEWORK DI SICUREZZA ↓ GDPR