

Network Security

Elements of Network Security Protocols

Organizzazione della rete

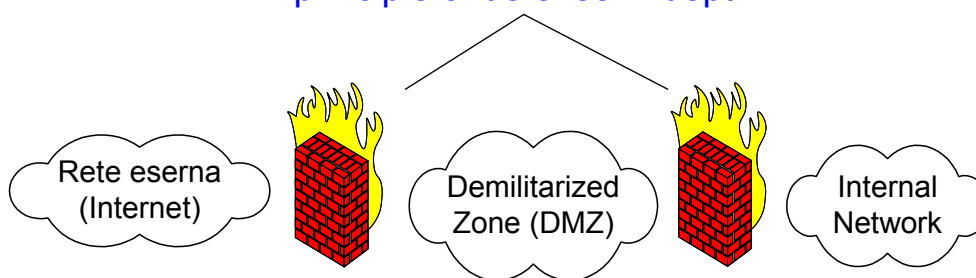
- Il firewall
- La zona demilitarizzata (DMZ)
- System security



- La principale difesa contro gli attacchi ad una rete è una corretta organizzazione topologica della rete stessa
- Uno dei principali approcci è quello di suddividere la rete in **zone di sicurezza**
 - i dispositivi e le risorse sono posizionati nelle zone in base ai loro livelli e requisiti di sicurezza
 - la rete acquisisce una maggiore scalabilità ed una conseguente maggiore stabilità

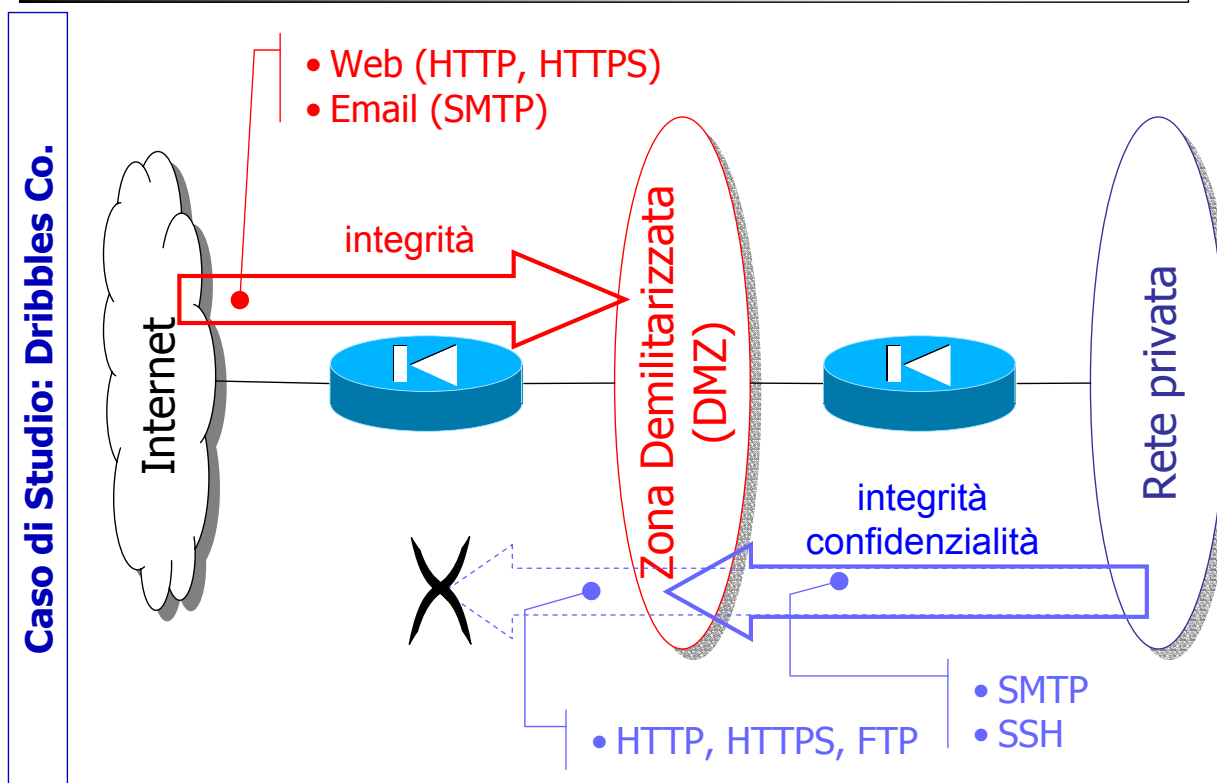


principle of defense in depth



- La zona demilitarizzata (DMZ) è una porzione di rete che separa la rete interna dalla rete esterna
- I server nella DMZ sono accessibili dalla rete pubblica, perciò non sono trusted (dalla rete interna) e quindi devono essere segregati rispetto a questa

se un server non è trusted allora la sua compromissione non dovrebbe avere effetti collaterali



Firewall: obiettivi e proprietà



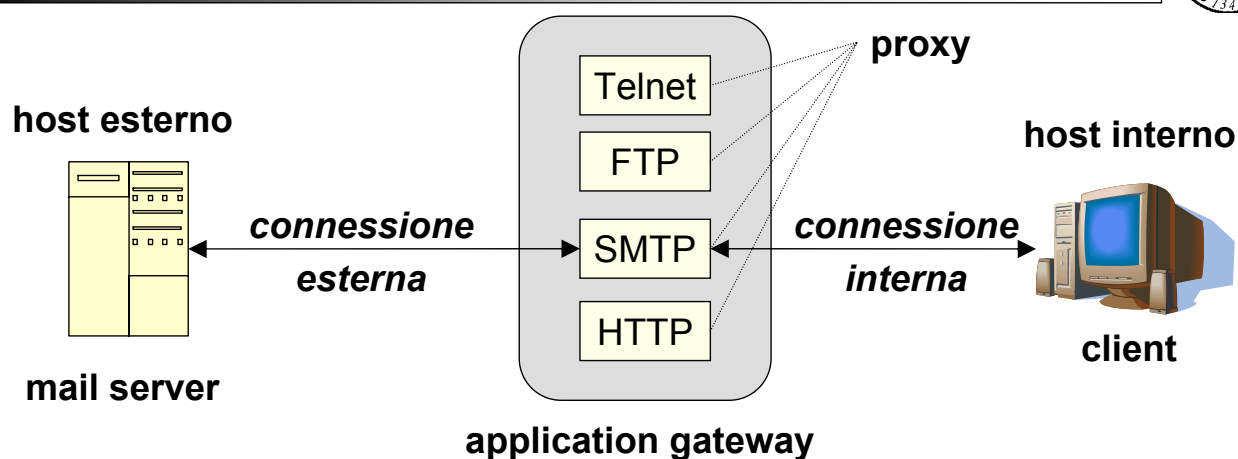
- Il Firewall è un dispositivo special purpose che impone una politica di controllo degli accessi tra due reti
- Il Firewall è posizionato tra le due reti con i seguenti obiettivi/proprietà:
 - tutto il traffico tra le due reti passa attraverso il firewall
 - solo il traffico autorizzato può passare
 - il firewall stesso è immune alla penetrazione
 - tutte le funzionalità sconosciute o di dubbia sicurezza possono essere eliminate (**principio di economia dei meccanismi**)
 - il firewall è amministrato meglio di un host
 - il firewall ha meno utenti di un host



- **Packet filter** viene installato a monte della rete protetta ed ha il compito di bloccare o inoltrare i *pacchetti IP* secondo *regole* definite a priori
- **Circuit/application gateway** analizza e filtra il traffico a livello trasporto/applicazione. Application gateway sfrutta la conoscenza del particolare servizio

Livello	Oggetto del monitoraggio	Funzione
<i>Application</i>	Data payload	Application gateway (proxy)
<i>TCP Transport</i>	TCP/UDP header	Circuit gateway
<i>IP Network</i>	IP header	Packet filtering

Application gateway



Vantaggi

- Autenticazione del cliente e del server
- Filtraggio specifico per il servizio di tutto il traffico
- Mascheramento della rete
- Logging

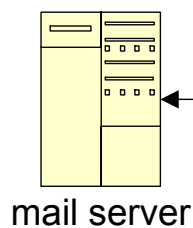
Svantaggi

- Non trasparente
- Un gateway per ogni servizio basato su TCP
- Reindirizzamento
- Carico aggiuntivo

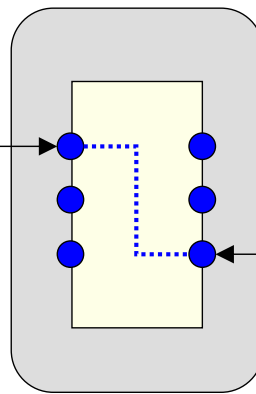
Circuit gateway



host esterno

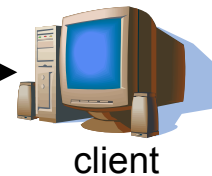


connessione
esterna



circuit gateway

host interno



connessione
interna

- Trasparente ma i client devono essere modificati
- Autenticazione del cliente e del server
- Autorizzazione, logging e caching delle connessioni
- Ripulitura della connessione

Proxy server



I servizi proxy hanno le seguenti caratteristiche

- i servizi proxy sono indipendenti tra di loro
- ciascun servizio proxy implementa solo un sottoinsieme delle funzionalità
- i servizi proxy sono pacchetti ridotti rispetto ai servizi
- un servizio proxy non accede al disco ad eccezione della lettura del suo file di configurazione
- ciascun servizio proxy viene eseguito come utente non privilegiato in una directory privata



- Il bastion host è un host critico per la sicurezza e costituisce la piattaforma per i gateway a livello di applicazione e di circuito

Il bastion host ha le seguenti caratteristiche

- monta un sistema operativo sicuro
- monta solo i servizi proxy necessari
- eroga ciascun servizio solo ad un sottoinsieme degli host della rete
- implementa forme di autenticazione aggiuntive e specifiche
- supporta logging & auditing



- Un packet filter (screening router) scarta o inoltra un pacchetto IP, da e verso la rete interna, sulla base di un insieme di regole di filtraggio
- Le regole di filtraggio si basano sul valore dei campi contenuti nell'intestazione IP e di trasporto (TCP/UDP) tra cui:
 - l'indirizzo del sorgente e del destinatario
 - il protocollo di trasporto
 - il numero di porta del sorgente e del destinatario
 - i flag SYN, ACK nell'header TCP
 - ...



- **exclusive policy (open system policy)**—la regola di default è **inoltrare**: ciò che non è espressamente proibito viene permesso
- **inclusive policy (closed system policy)**—la regola di default è **scartare**: ciò che non è espressamente permesso viene proibito

Regole



- Un firewall applica un insieme di regole; ogni regola ha la seguente struttura (IPF*-like)
 - action options selection [flags keep state]**
- il campo **action** specifica cosa fare con un pacchetto che soddisfa la regola di selezione
- il campo **selection** specifica la regola di selezione dei pacchetti
- il campo **options** specifica
 - l'interfaccia (**on interface**) su cui applicare la regola di selezione,
 - se la regola di selezione deve essere applicata ai pacchetti in ingresso (**in**) o in uscita (**out**)
- i campi **flags** e **keep state** saranno discussi più avanti

* IPF (IPfilter Firewall); per brevità, nelle regole seguenti, la keyword **quick** è omessa



- **block in on dc0 proto tcp/udp from UnIP to any**
–bloccare tutto il traffico entrante proveniente da *UnIP*
- **pass in on dc0 proto tcp from any to MioIP port = 25**
–passare il traffico di email destinato a *MioIP*
- **pass out on dc0 proto tcp from any to any port = 25**
–passare il traffico di email in uscita
- **block out log on dc0 all** –bloccare tutto il traffico in uscita (default)
- **block in log on dc0 all** –bloccare tutto il traffico in ingresso (default)

Stateful packet filtering (cont.)



- Si autorizzano i pacchetti in uscita verso la porta 80 di un qualunque host

pass out on dc0 proto tcp from any to any port = 80

- Si autorizzano i pacchetti in ingresso provenienti dalla porta 80 di un qualunque host

pass in on dc0 proto tcp from any port = 80 to any

- *Attenzione: non c'è nessuna garanzia che un pacchetto proveniente dalla porta 80 di un host esterno sia stato inviato dal servizio WWW*

Stateful packet filtering (cont.)



- Lo stateful filtering considera il traffico come uno scambio bidirezionale di pacchetti IP che costituisce una *sessione di conversazione (conversation session)*
- Lo stateful filtering permette di *generare dinamicamente le regole per il prossimo pacchetto* (anche ICMP) nella sessione di conversazione
- In uscita/ingresso, se un pacchetto soddisfa il criterio di selezione della regola dinamica, il pacchetto viene lasciato passare e viene generata la regola per il prossimo pacchetto; altrimenti al pacchetto sono applicate le regole statiche
- Lo stateful filtering permette di concentrarsi sul passare o bloccare una nuova sessione: i successivi pacchetti della sessione subiranno la stessa sorte

Stateful packet filtering (cont.)



▪ Outbound traffic

allow out non-secure standard www function

pass out on dc0 proto tcp from any to any port = 80 **flags S keep state**

▪ Inbound traffic

allow in standard www function

pass in on dc0 proto tcp from any to any port = 80 **flags S keep state**

- **Keep state**—la parola chiave **keep state** in una regola **pass** attiva lo stateful filtering se un pacchetto soddisfa il criterio di selezione
- **Flag S**—il **flag S** specifica un pacchetto che trasporta un tcp connection request

Stateful packet filtering (cont.)



- *allow out access to my ISP's DNS*

pass out on dc0 proto **tcp** from any to *ISP* port = 53 **flags S keep state**

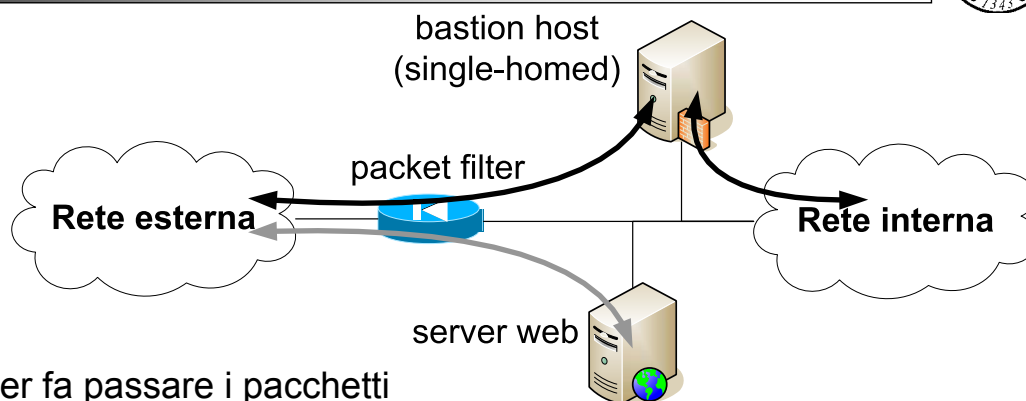
pass out on dc0 proto **udp** from any to *ISP* port = 53 **keep state**

- *allow access to my ISP's DHCP Server*

pass out on dc0 proto **udp** from any to *ISP* port = 67 **keep state**

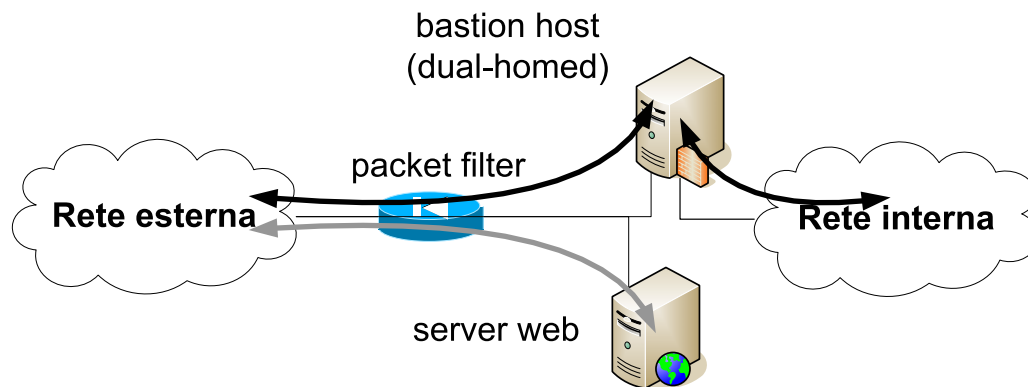
pass in on dc0 proto **udp** from *ISP* to any port = 68 **keep state**

Screened host firewall (single-homed)



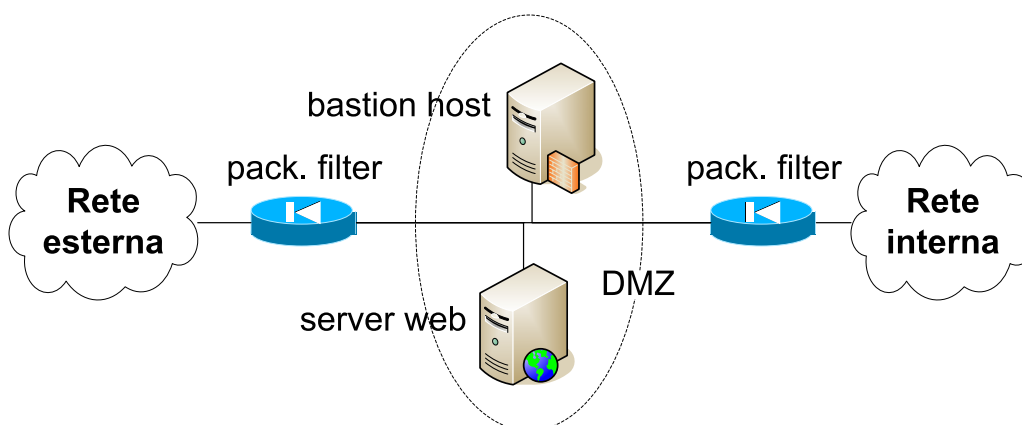
- il packet filter fa passare i pacchetti provenienti dall'esterno e diretti al bastion host
- il packet filter può far passare i pacchetti provenienti dall'esterno e diretti ad un server che non ha un livello di sicurezza elevato (es. server web)
- il packet filter fa passare i pacchetti provenienti dal bastion host e diretti verso l'esterno
- **il traffico viene analizzato due volte**, ma se il packet filter viene compromesso, il traffico esterno può raggiungere la rete interna

Screened host firewall (dual-homed)



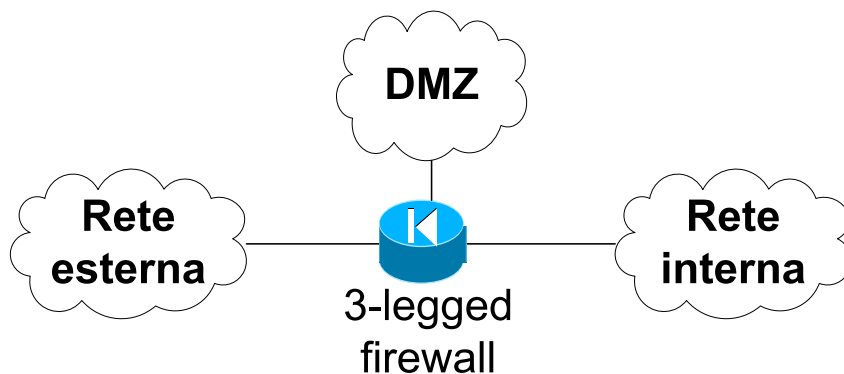
- il dual-homed bastion host previene i problemi causati dalla compromissione del packet filter perché un pacchetto deve “fisicamente” attraversare il bastion host

Screened subnet firewall



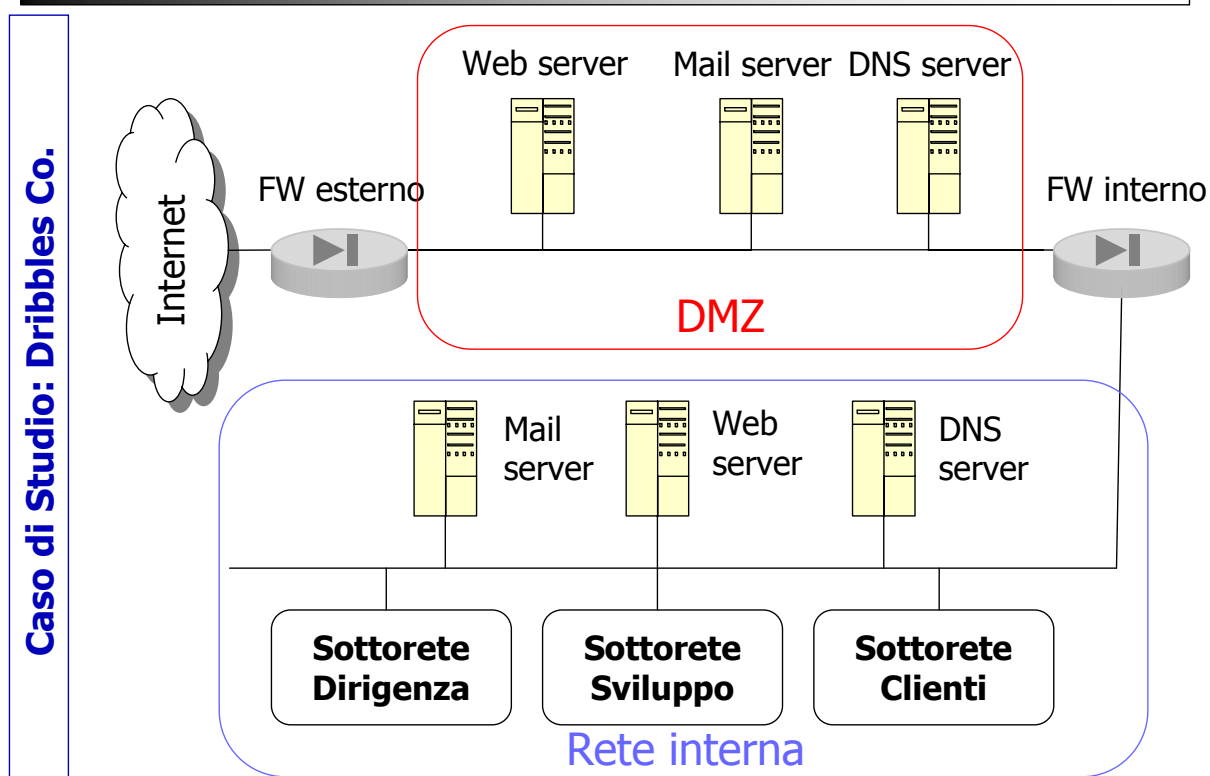
- È l'architettura più sicura delle tre
- La DMZ è accessibile sia dalla rete interna sia dalla rete esterna
- Il traffico non può attraversare la DMZ

Three-legged architecture



- Il firewall deve avere tre interfacce
- la DMZ rimane isolata dalla rete interna


Organizzazione della rete





- La politica di sicurezza prevede che
 - certe informazioni aziendali siano rese disponibili all'esterno
 - dall'esterno non è possibile comunicare direttamente con gli host nella rete interna
 - gli host della rete interna non possono comunicare direttamente con l'esterno
- La DMZ fa da "pompa" e regola le informazioni che escono dall'interno



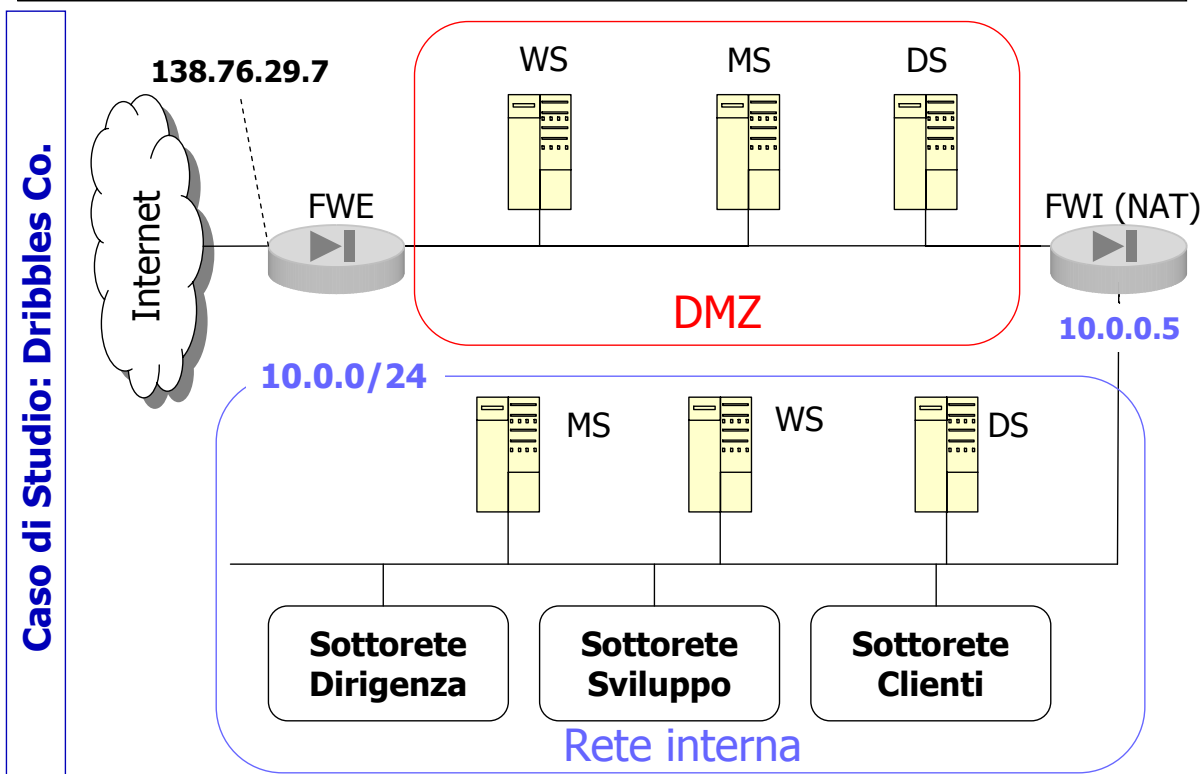
- Selezionare il target
- Identificare i sistemi da attaccare
- **Ottenere informazioni** 
 - Attraverso la rete
 - Banner scanning
 - Network profiling (nmap, nessus, ...)
- Ottenere l'accesso
- Acquisire privilegi
- Evitare la scoperta
- Realizzare l'obiettivo

Il processo di hacking



The image shows two browser windows. The left window displays a security report for a port, listing DCE services with their UUIDs and endpoints. A red circle highlights the 'smtp (25/tcp)' entry. The right window shows the NeWT plugin page for 'SMTP Server type and version', detailing its function, version (10263), and a solution to change the login banner.

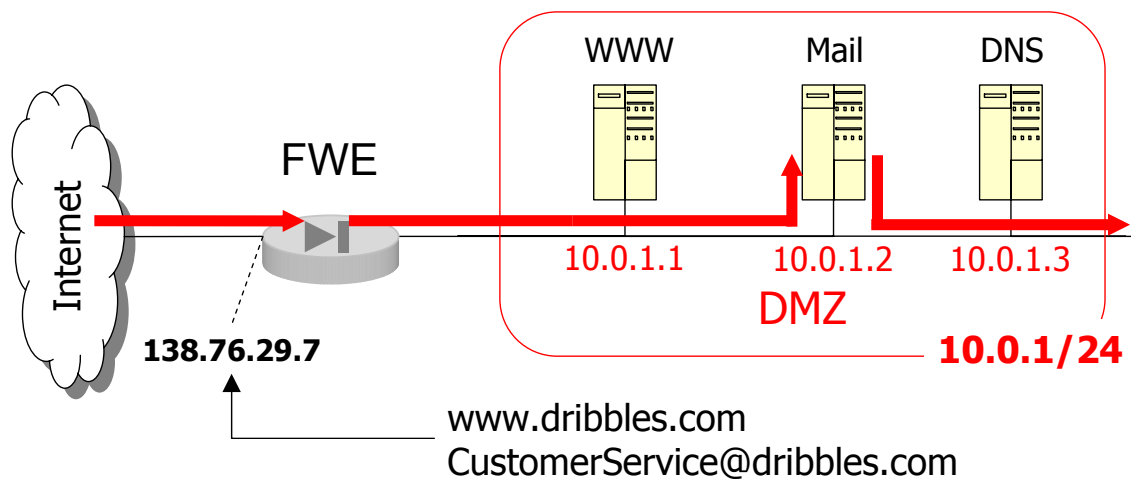
Proteggere gli indirizzi della rete interna



Il firewall esterno (cont.)



Caso di Studio: Dribbles Co.



- FWE permette traffico in ingresso di tipo SMTP, HTTP[S], [DNS]
- Dall'esterno si "vede" solo l'indirizzo IP di FWE
- I server in DMZ sono dei gateway
(si assume che FWE svolga anche "limitate" funzioni di gateway)

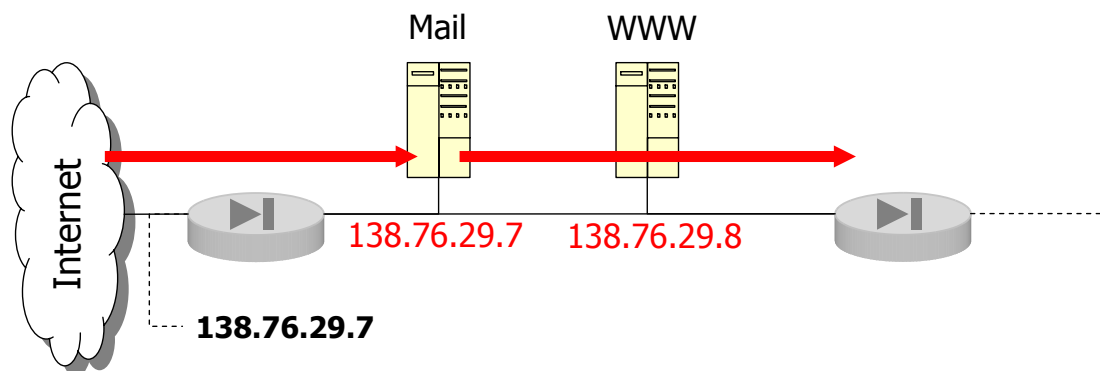
Network Security

29

Il firewall esterno



Caso di Studio: Dribbles Co.



- **Sicurezza limitata** in quanto gli indirizzi interni sono visibili
- **Scalabilità limitata** in quanto non è possibile alcuna forma di distribuzione del carico ed è possibile solo una limitata riconfigurabilità

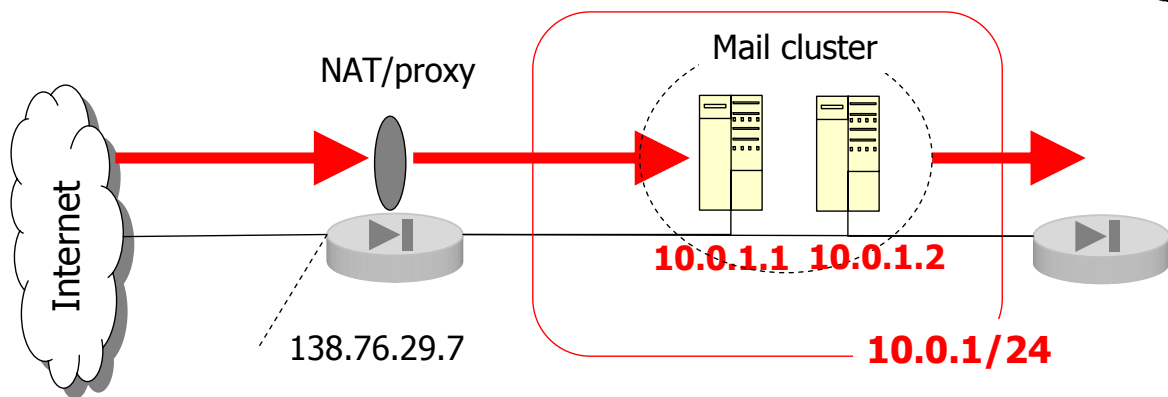
Network Security

30

Il firewall esterno



Caso di Studio: Dribbles Co.



- Maggiore sicurezza
- Maggiore scalabilità

Il Firewall interno



Caso di Studio: Dribbles Co.

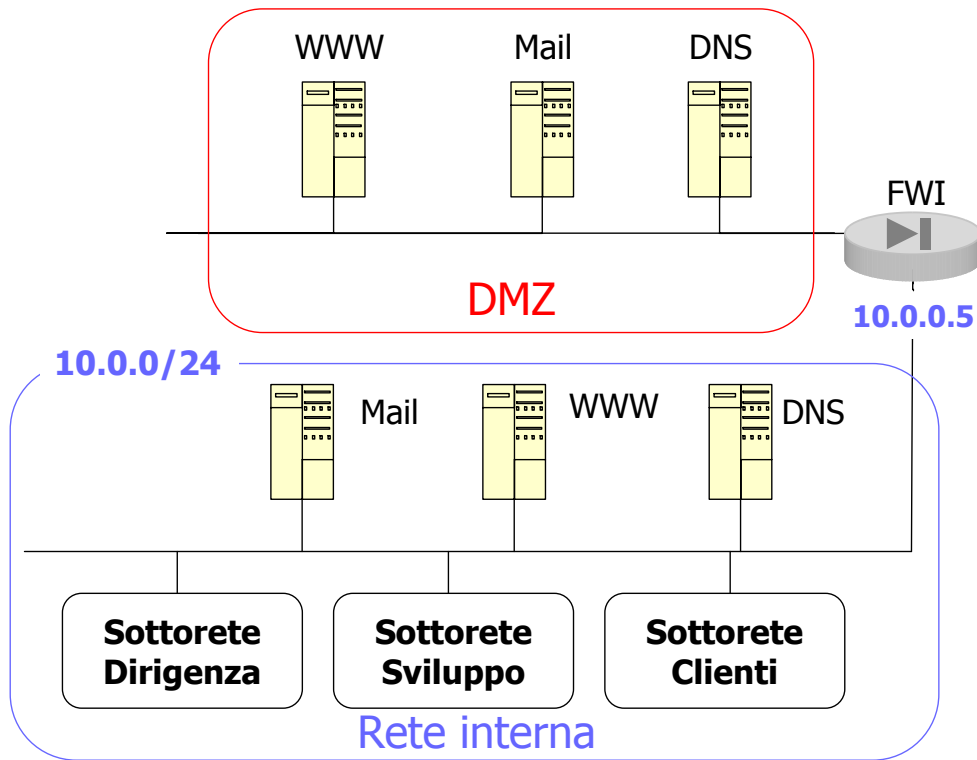
Il firewall interno deve

- permettere la connessione tra il mail server interno ed il mail server in DMZ
- permettere la connessione al DNS in DMZ
- permettere le connessioni SSH verso i server della DMZ

Il firewall interno



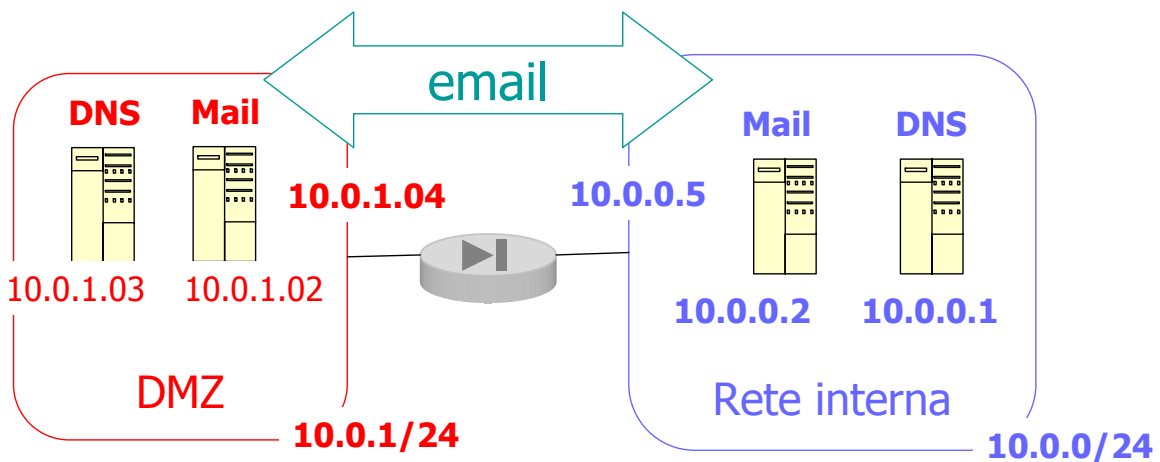
Caso di Studio: Dribbles Co.



Il firewall interno



Caso di Studio: Dribbles Co.



Mail Server in DMZ deve conoscere un indirizzo per il Mail Server Interno e viceversa

Non è necessario che questi indirizzi siano i reali indirizzi dei server ma possono essere indirizzi fittizi che il firewall riconosce

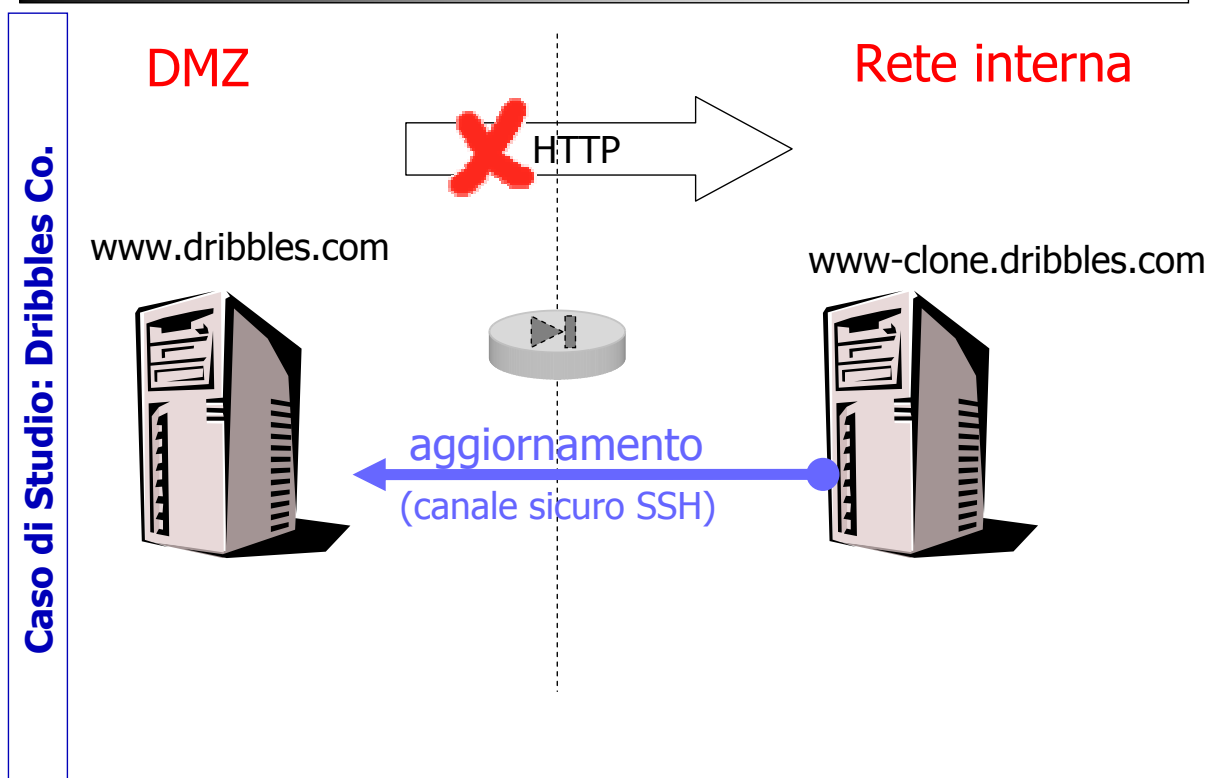
Questi indirizzi possono essere fissi oppure si può utilizzare il DNS

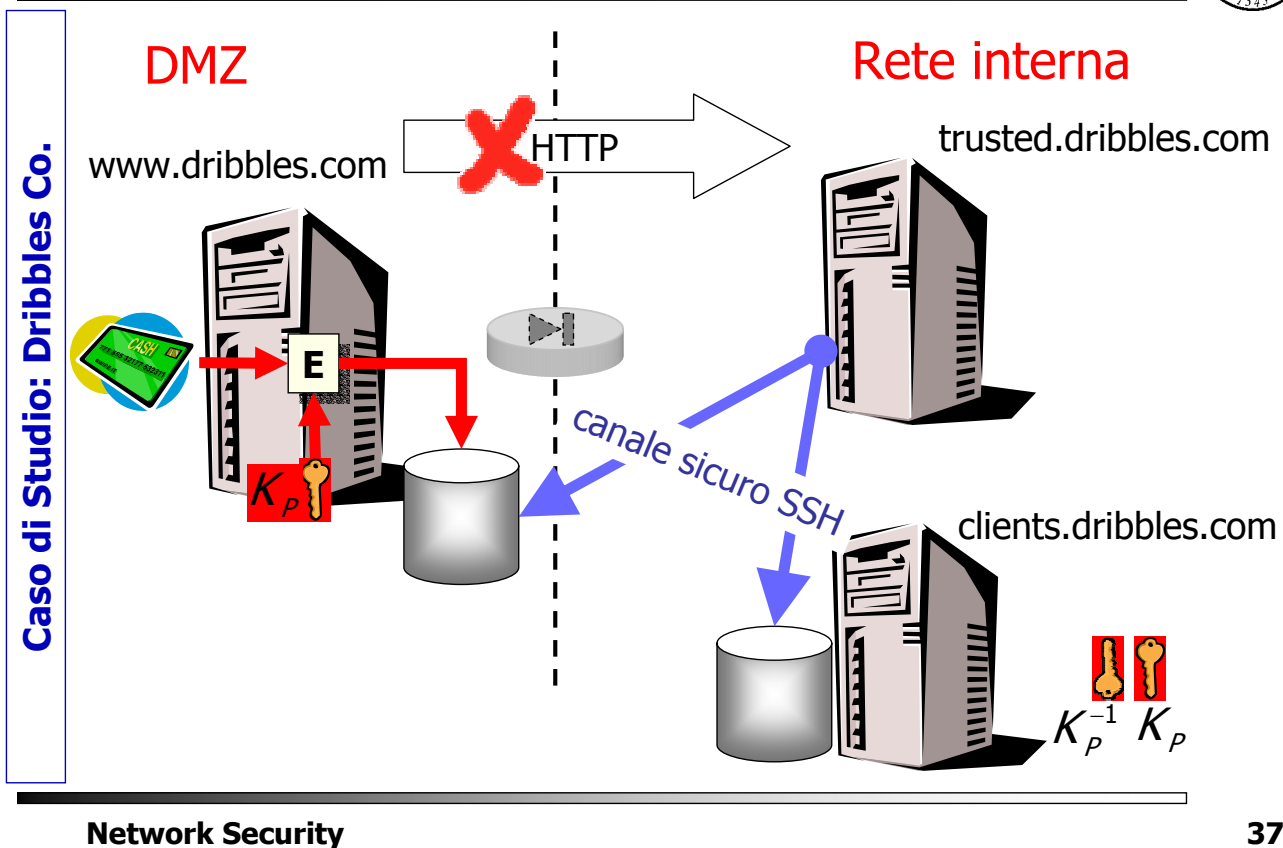
Il Mail Server in DMZ



- Il mail server (proxy) ha il compito di analizzare e bonificare il contenuto e gli indirizzi di ogni messaggio di email; il firewall deve perciò compiere solo controlli rudimentali
- **Quando riceve un email**
 - a) il proxy ricostruisce l'email (header, body ed attachments), riporta gli attachment nella loro forma nativa ed analizza l'email e gli attachment così ottenuti
 - b) il proxy riporta l'email in formato SMTP e la ricontrolla
 - c) sulla base del destinatario, il proxy inoltra l'email al mail server interno
- **Quando invia un email**
 - a) il proxy esegue gli stessi passi a) e b); il passo c) è diverso. Al passo b) cerca informazioni proprietarie e sensibili
 - c) il proxy scandisce l'header, qualunque informazione relativa ad indirizzi/nomi interni è cancellata o riscritta

WWW server in DMZ

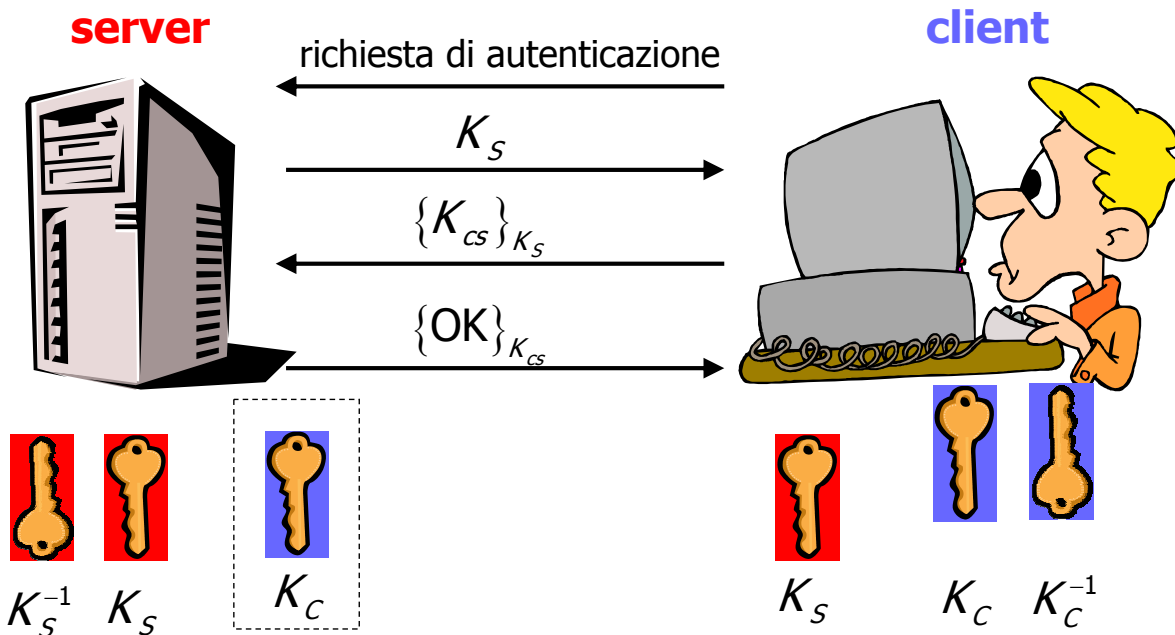




SSH

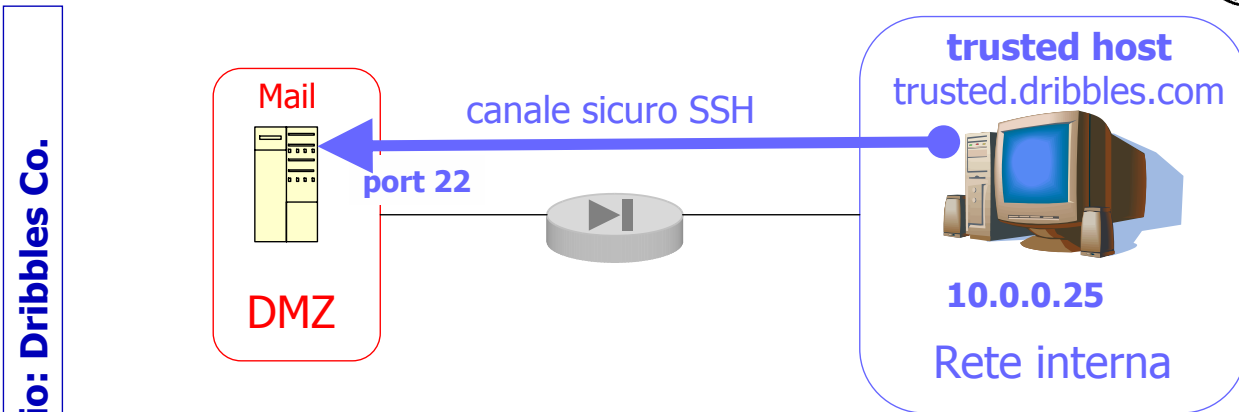


- SSH permette di operare su di una macchina remota in modo sicuro
- È stato concepito per rimpiazzare gli r-tools
- SSH fornisce *two-way authentication* e permette di stabilire una connessione sicura (confidenzialità ed integrità) con la macchina remota
- SSH opera su TCP ed utilizza come porta d'ascolto la porta 22



Il client può essere autenticato dal server tramite password oppure tramite la sua chiave pubblica

Connessioni SSH



Caso di Studio: Dribbles Co.

- La connessione SSH è diretta e non mediata da un proxy. Tuttavia,
- il firewall garantisce che la connessione sia originata da un host interno trusted e sia diretta solo a server in DMZ
- solo gli amministratori di rete hanno accesso al trusted host
- il canale SSH è sicuro



- DNS contiene le entrate nome-indirizzo necessarie ai server in DMZ e cioè le entry relative a:
 - web server, mail server e log server in DMZ
 - trusted administrative host
 - firewall esterno (per mail transfer)
 - firewall interno (per mail transfer)
- DNS in DMZ non conosce gli indirizzi del mail server interno
- DNS deve essere aggiornato solo se cambia l'indirizzo del trusted administrative host

