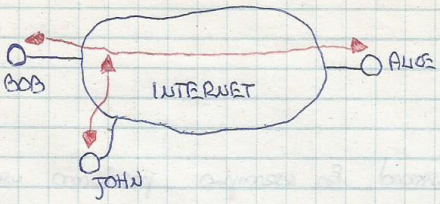
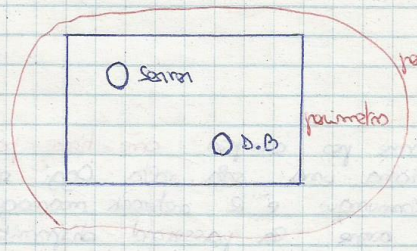
Concludiamo parlando di sicurezza. Consideriamo la seguente situazione:



John può intercettare la comunicazione tra Bob e Alice. Esistono fondamentalmente due tecniche per evitare ciò:

- end to end encryption
- tunnelling IP

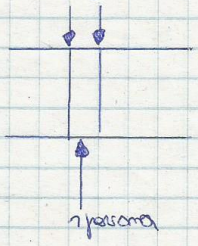
Il tunnelling IP l'abbiamo già analizzato. Nelle aree più critiche cioè nelle aree dove ci sono i servizi più critici si ricorre alla sicurezza fisica (physical Security).



NB: Il perimetro più interno è un perimetro ad alta sicurezza.

Il perimetro interno deve avere tutta una serie di caratteristiche tra cui:

1) numero limitato di accessi
2) Accessi controllati da porte comandate da Smart Card.
3) Porte doppie

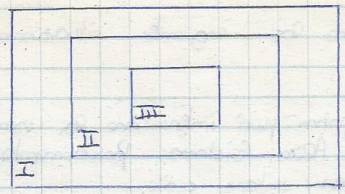


4) Il perimetro deve essere realizzato con muri contenenti una schermatura di piombo (gabbia di Faraday). I segnali radio non si devono propagare al di fuori del perimetro stesso.

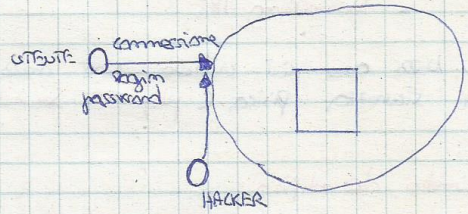
5) I cavi che collegano il perimetro interno al perimetro esterno sono così fatti:

TUBO CON GAS INTERNO.

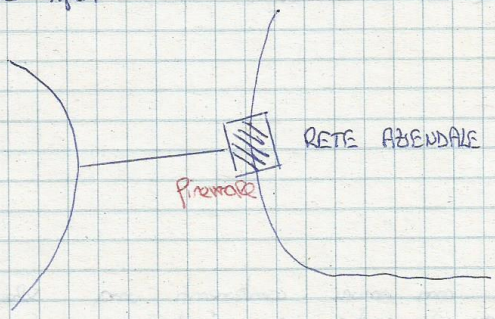
Un altro problema, non da poco, che bisogna gestire è l'accesso da parte di persone provenienti da altre aziende. In merito si divide l'edificio in zone di livello sempre più critiche.



Tale accesso può essere regolamentato da password. Per esempio possiamo usare una semplice password:



oppure possiamo usare password speciali come per esempio one-time-password che altro non è che una password che funziona una sola volta. Oggi si usano le password generator (con interfaccia USB). Comunque è il network manager che svolge la fase di configurazione in modo tale da avere la password disponibile per ogni accesso. Infine ci sono le password biometriche come per esempio password che sfruttano la scansione della retina o la scansione delle impronte digitali. Quest'ultime password sfruttano i cosiddetti sistemi PR (Pattern Recognition). Questi sistemi sono sistemi di riconoscimento di pattern ossia sistemi di riconoscimento di oggetti che rappresentano determinati fenomeni fisici. Supponiamo ora di avere una situazione di questo tipo:

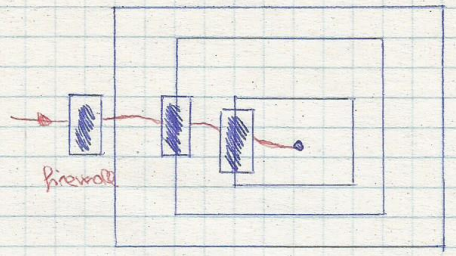


Un firewall è una "strumento" che controlla i pacchetti in ingresso ed esegue il filtraggio. Il filtraggio può essere di tre tipi:

1) filtraggio su base utente (filtraggio su S.A, login, password).
2) filtraggio su servizio (sfruttando porte TCP/UDP)
3) filtraggio a livello applicativo (verifica per esempio del tipo di payload).

Quindi un'azienda che ha una o più connessioni esterne deve installare un firewall su ciascuna di esse e poi coordinare tutti i firewall. Abbiamo visto che una azienda viene suddivisa in zone in base alla criticità dei servizi forniti dai vari livelli.

Di conseguenza anche le risorse all'interno dell'azienda sono suddivise per livelli.



CASCATA DI FIREWALL

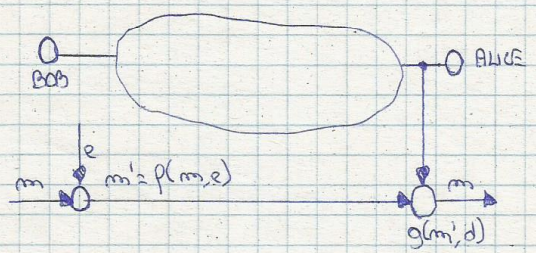
Vediamo ora la configurazione dei firewall. Tale operazione è abbastanza critica e pesante. Bisogna:

1) specificare cosa è vietato
2) specificare cosa è permesso

Il secondo tipo di specifica è più stringente. L'approccio numero uno è pericoloso ma è veloce. L'approccio numero due è sicuro, ma è più costoso come gestione. Parliamo ora brevemente anche dell'encryption. I sistemi di criptazione/decriptazione si basano su due tipi di algoritmi:

1) algoritmi a chiave privata
2) algoritmi a chiave pubblica

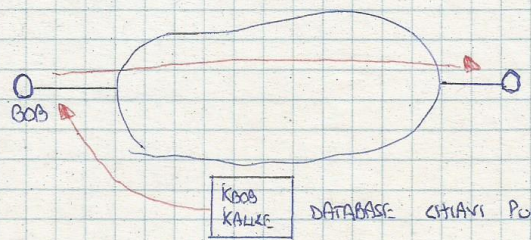
Gli algoritmi a chiave privata, come per esempio DES, sono semplici da gestire ed hanno una connessione simmetrica di tipo PUNTO - PUNTO.



CHIAVI: e = encryption
d = decryption

Tale algoritmo è efficiente e le chiavi possono essere a 122 o 168 bit.

Gli algoritmi a chiave pubblica invece sono algoritmi asimmetrici e si basano su funzioni difficilmente invertibili.



DATABASE CHIAVI PUBBLICHE.

Un esempio di tale algoritmo è RSA.

SCHEMI:

* Protocollo ARP:

0	16	31
HARDWARE TYPE		PROTOCOL TYPE
HLEN	PLEN	OPERATION
SENDER HA		
SENDER HA		SENDER IP
SENDER IP		TARGET HA
TARGET HA		
TARGET IP		

32 bit.

Hardware type = specifica il tipo di interfaccia hardware usata (per ETHERNET è 1).
Type Protocol = tipo di indirizzo ad alto livello che il mittente ha fornito (0800_{16}).
Operation = specifica il tipo di operazione (richiesta, o risposta).
HLEN e PLEN = specificano lunghezza dell'indirizzo hardware e dell'indirizzo IP.
SENDER HA, SENDER IP = indirizzo hardware e IP del mittente
TARGET HA, TARGET IP = indirizzo hardware e IP della macchina di destinazione.

* PACCHETTO IP:

HEADER	PAYLOAD.

IPv4

L'header è composto da:

4	4	8	16
VERSIONE	HLEN	TOS	TOTAL LENGTH
IDENTIFICATION		FLAGS (3 bit)	FRAGMENT OFFSET (13 bit)
TTL		PROTOCOL	HEADER CHECKSUM
S.A (SOURCE ADDRESS)			32 bit
D.A			32 bit

16 bit

20 byte di Header. TOS = Type of service: PPP, DTR, (XX)

* Msg ICMP:

1) ICMP ECHO REQUEST AND REPLY MESSAGE

8	8	16
TYPE	CODE	CHECKSUM
IDENTIFIER		SEQUENCE NUMBER
OPTIONAL DATA		

CODE = 0
TYPE = 8 REQUEST
= 0 REPLAY

2) ICMP UNREACHABLE DESTINATION:

8	8	16
TYPE	CODE	CHECKSUM

{ TYPE = 3
{ CODE = varia

3 parole che contengono header del pacchetto IP.

64 bit iniziali del PAYLOAD del pacchetto IP.

3) ICMP TTL EXPIRED:

TYPE	CODE	CHECKSUM
header del pacchetto IP + primi 64 bit dopo header.		

{ TYPE = 11
{ CODE = 0 EXPIRED
= 1 riassemblaggio TIMEOUT EXPIRED.

4) ICMP CLOCK SYNCHRONIZATION & TRASMIT TIME ESTIMATION

TYPE	CODE	CHECKSUM
IDENTIFICATORE		SEQUENCE NUMBER
ORIGINATE TIME STAMP		
RECEIVE TIME STAMP		
TRANSMIT TIME STAMP		

{ CODE = 0
{ TYPE = 13 richiesta
= 14 risposta

5) ICMP ROUTER SOLICITATION

TYPE = 9	CODE = 0	CHECKSUM
#INDIR.	ADD SIZE	LIFETIME
ROUTER ADDRESS 1		
PREFERENCE LEVEL #1		
ROUTER ADDRESS 2		
PREFERENCE LEVEL #2		

} elenco dei router dichiarati

* MESSAGGI RIP 2:

COMMAND	VERSION	ROUTING DOMAIN
FAMILY OF NETWORK 1		ROUTE TAG NET 1
IP ADDRESS OF NET 1		
SUBNET MASK OF NET 1		
NEXT HOP NET 1		
DISTANCE TO NET 1		
. . . . .		

* MESSAGGI OSPF:

VERSIONE	TYPE	MESSAGE LENGTH
SOURCE ROUTER IP ADDRESS		
AREA ID		
CHECKSUM	AUTENTICAZIONE	
AUTENTICAZIONE		
AUTENTICAZIONE		

• LSA UPDATE:

Header:

LINK AGE	LINK TYPE
LINK ID	
ADVERTISING ROUTER	
LINK SEQUENCE NUMBER	
CHECKSUM	LENGTH

* MESSAGGI BGP:

MARKER 16 byte		
LENGTH 2byte	TYPE 1byte	

msg BGP OPEN

VERSIONE
AS NUMBER
HOLD TIME
BGP IDENTIFIER
PATH LENGTH
PARAMETR

msg BGP UPDATE

WITH DRAW LENGTH	
WITH DRAW DESTINATION	
PATH LENGTH	
PATH ATTRIBUTES	
DESTINATION NETWORKS	

* MESSAGGI IGMP:

TYPE	RESPONSE TIME	CHECKSUM
MULTICAST GROUP ADDRESS		

- TYPE = JOIN GROUP
  = LEAVE GROUP

* MESSAGGI BOOTP:

OPERATION	HTYPE	HLEN	HOPS
TRANSACTION ID			
SECONDS	–		
CLIENT IP ADDRESS			
YOUR IP ADDRESS			
SERVER IP ADDRESS			
ROUTER IP ADDRESS			
CLIENT HARDWARE ADDRESS			
CLIENT HOST NAME			
SERVER HOST NAME			
BOOT FILENAME			
VENDOR SPECIFIC AREA			

→ identifica la transazione

→ specifica il numero di secondi trascorsi da quando il client ha iniziato la procedura di BOOTSTRAP.

* CARE-OF-ADDRESS:

TYPE	----	----
LIFETIME		
CARE OF ADDRESS		

* HEADER UDP:

SOURCE PORT	DESTINATION PORT
LENGTH	CHECKSUM
PAYLOAD DATA A LIVELLO APPLICATIVO	

* HEADER TCP:

SOURCE PORT			DESTINATION PORT
SEQUENCE NUMBER			
ACK NUMBER			
HLEN	-	FLAGS	WINDOW
CHECKSUM			URGENT POINTER

* MESSAGGIO ICMP PER DISCOVERY MOBILE IP

TYPE = 16	LENGTH	SEQUENCE NUMBER	
LIFETIME		CODE = 7	-
CARE-OF-ADDRESS			

*