Contromisure

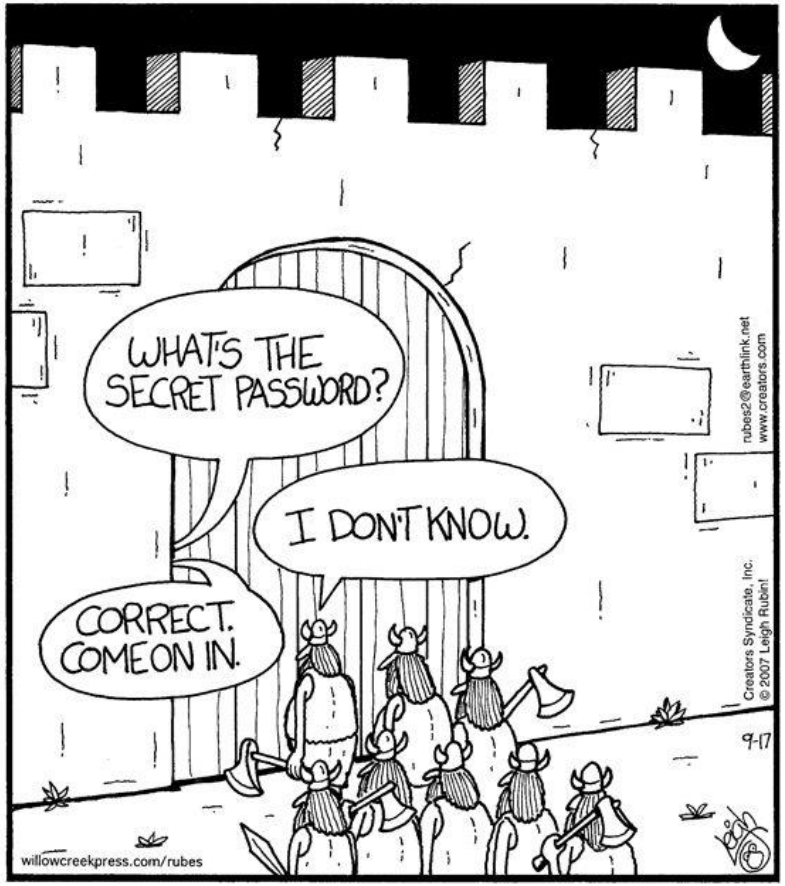
Contromisure

- Gestione degli accessi al sistema(autenticazione) e ai locali
- Antivirus
- Analisi del traffico di rete (Firewall, IDS/IPS)
- Analisi utilizzo delle risorse di sistema, accessi (IDS/IPS)
- Backup dati locale e remoto
- Gruppi di continuità(in caso di blackout, sbalzi di tensione,…), sistemi antincendio, autodiagnosi problemi hardware…
- Protezione dell'informazione (Crittografia - Steganografia - Firme digitali)
- Politiche di sicurezza, formazione del personale

Contromisure: efficacia

- Consapevolezza del problema: gli utenti del sistema devono essere convinti della necessità di sicurezza
- Consapevolezza della vulnerabilità: adeguata formazione del personale
- Probabilità d'uso: nessuna misura è utile se non è utilizzata
- Sovrapposizione dei controlli: diversi controlli possono essere applicati contemporaneamente per evitare un possibile danno
- Revisione Periodica: pochi controlli hanno un'efficacia permanente

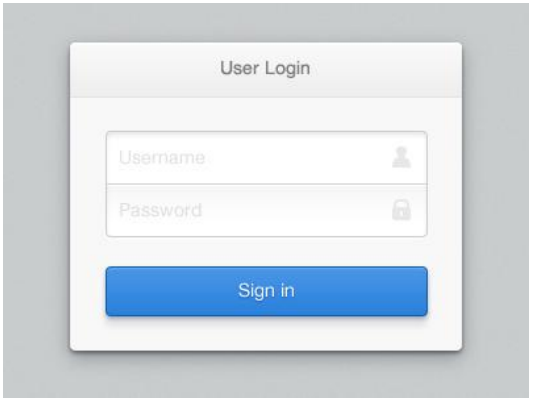
Contromisure: efficacia

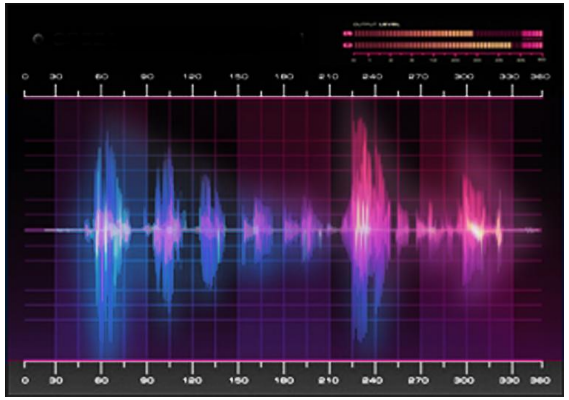


Why great care and consideration should be taken when selecting the proper password

Contromisure: autenticazione

- Username e Password
- Tessere magnetiche o elettroniche, pen drive,…
- Analisi biometriche: impronte digitali, riconoscimento vocale, scansione retina, vene della mano,…





Contromisure: password

Le password possono essere:

- Intercettate(sniffing)
- Indovinate
- Ottenute grazie a tecniche di ingegneria sociale
- Rubate(keylogger, phishing, spyware, memo, …)
- Ottenute grazie ad attacchi a dizionario (elenco di password comuni)
- Ottenute grazie ad attacchi a forza bruta (provando tutte le combinazioni possibili o quantomeno quelle più probabili)
- E' possibile decodificare anche password criptate se si conosce l'algoritmo (es. MD5) provando le varie combinazioni o effettuando una ricerca su Google!!
- Si possono cambiare (forget your password?)

Contromisure: password

Il numero di combinazioni possibili cresce esponenzialmente con il numero di caratteri della password (prima figura) e con il numero di caratteri del set utilizzato (seconda figura)

caratteri	nr car nel set	tentativi/sec	car. pwd	nr totale di pwd	giorni	anni
a-z A-Z 0-9	62	1,000,000	5	916,132,832	0.0	0.00
a-z A-Z 0-9	62	1,000,000	6	56,800,235,584	0.7	0.00
a-z A-Z 0-9	62	1,000,000	7	3,521,614,606,208	40.8	0.11
a-z A-Z 0-9	62	1,000,000	8	218,340,105,584,896	2527.1	6.92
a-z A-Z 0-9	62	1,000,000	9	13,537,086,546,263,600	156679.2	429.26

caratteri	nr car	tentativi/sec	car. pwd	nr totale di pwd	giorni	anni
a-z	26	1.000.000	7	8.031.810.176	0,1	0,00
a-z A-Z	52	1.000.000	7	1.028.071.702.528	11,9	0,03
a-z A-Z 0-9	62	1.000.000	7	3.521.614.606.208	40,8	0,11
a-z A-Z 0-9 !£@	95	1.000.000	7	69.833.729.609.375	808,3	2,21
a-z A-Z 0-9 !£@ non stampa	127	1.000.000	7	532.875.860.165.503	6167,5	16,90

Contromisure: password

Come scegliere password sicure? In generale valgono i seguenti criteri:

- Almeno 8 caratteri alfanumerici(con maiuscole, minuscole, numeri e segni di interpunzione)
- Nessuna informazione personale
- Nessuna parola del dizionario
- Complesse ma semplici da ricordare

Per approfondire…

Contromisure: Antivirus

Contromisure: Antivirus

- Programma che serve a rilevare la presenza di virus ed altri tipi di malware, ad impedire l'esecuzione dei file infetti ed eventualmente a rimuovere il malware o cancellare i file stessi
- Effettua una scansione dei file cercando di individuare le «firme» dei malware che conserva in un database costantemente aggiornato
- …e attraverso una serie di «euristiche» che permettono di rilevare anche virus «polimorfi»

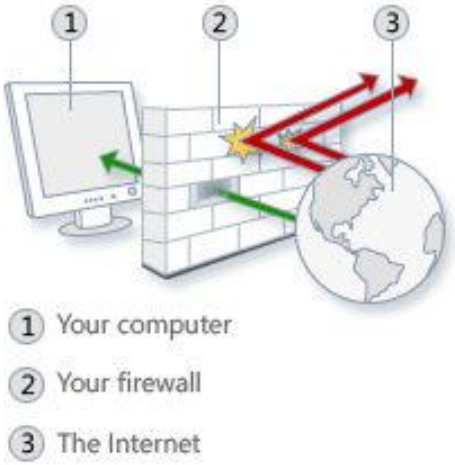
Contromisure: Antivirus

- Gli antivirus permettono sostanzialmente di rilevare solo le minacce conosciute (di cui si siano individuate le «firme»)
- Anche se gli antivirus di nuova generazione sono in grado di riconoscere e classificare come malware un programma anche sulla base del suo comportamento…
- La ricerca basata su «euristiche» consiste nel cercare istruzioni sospette perché tipiche del comportamento dei virus (come la ricerca di file o routine di inserimento all'interno di un altro file)

Firewall di rete

Funzione

Filtra il traffico in ingresso e in uscita dalla rete analizzando indirizzo IP e numero di porta

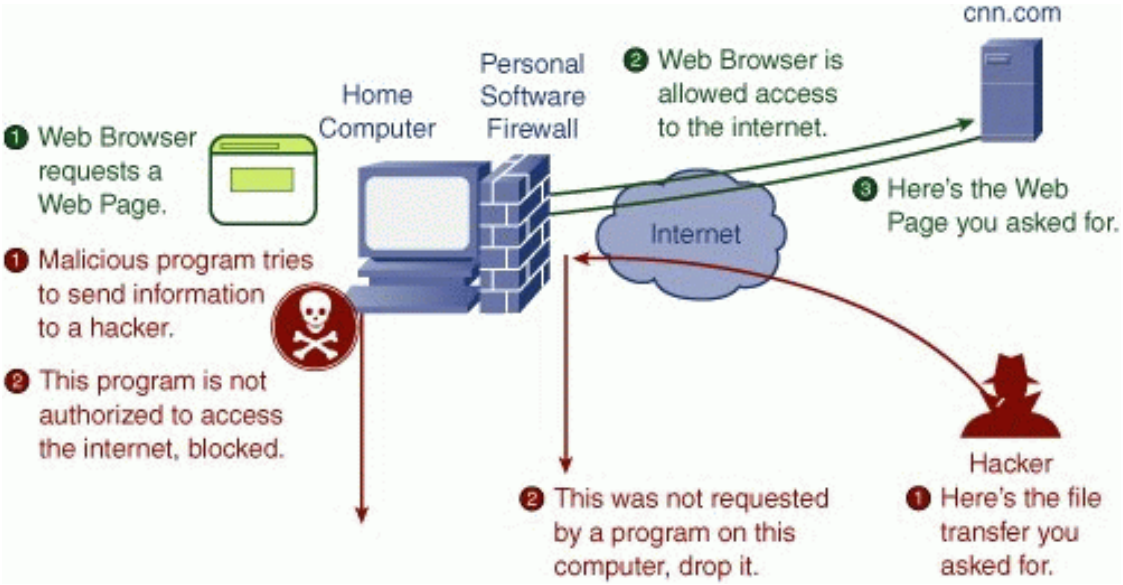


Limitazioni

- può facilmente essere aggirato semplicemente modificando l'IP in maniera che i pacchetti «sembrino» provenire da un server sicuro…
- Inoltre la maggior parte degli attacchi arrivano dall' «interno» della rete

Personal Firewall

Determina quali applicazioni possono trasmettere/ricevere dati attraverso internet

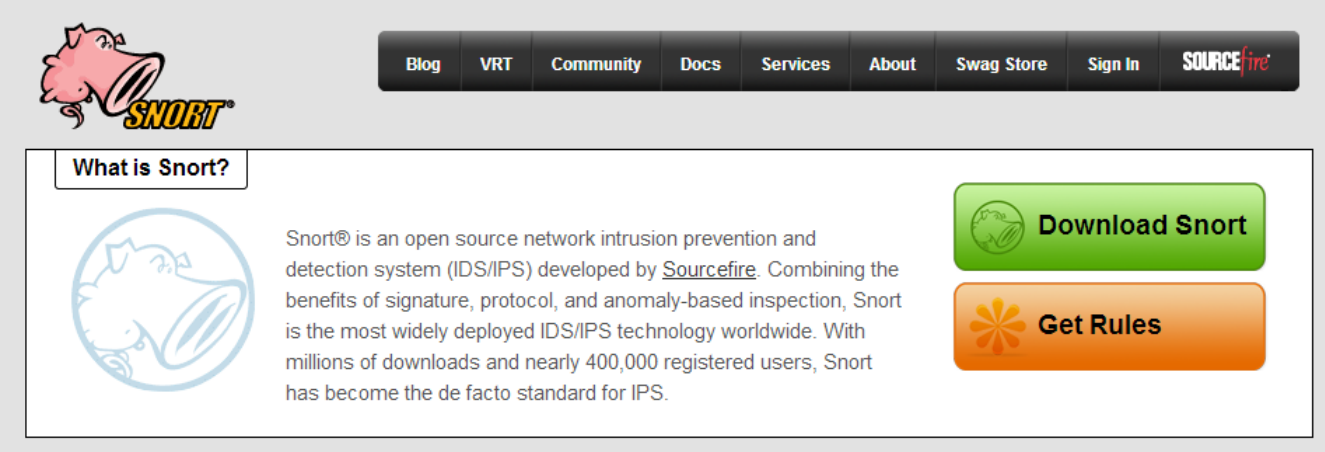


Personal Firewall

Fonte	Destinazione		Azione	Descrizione
indirizzo	indirizzo	porta		
192.168.0.1	any	80	allow	traffico web
192.168.0.2	any	80	allow	traffico web
192.168.0.2	any	21	allow	traffico ftp
any	192.168.0.10	25	allow	posta elettronica
any	192.168.0.x	135	Deny	Netbios
192.168.0.x	any	>1023	Deny	altri servizi

Contromisure: IDS e IPS

- IDS (Intrusion Detection System) si occupano di monitorare ed analizzare in tempo reale il traffico di rete e le attività eseguite da un sistema, rilevando eventuali anomalie
- IPS (Intrusion Protection System) oltre a svolgere le funzioni dell'IDS…
  - cercano di identificare la fonte dell'attività rilevata
  - registrano e segnalano eventuali violazioni o operazioni sospette
  - Tentano di bloccare l'intrusione



Contromisure: IDS e IPS

Gli IDS servono in quanto…

- Gli antivirus sono in grado di rilevare solo i virus conosciuti
- Le password possono essere indovinate/estorte con l'inganno/rubate/cambiate
- I firewall «tradizionali» non sono in grado di rilevare gli attacchi né tantomeno di bloccarli per le limitazioni prima evidenziate

Al contrario gli IDS…

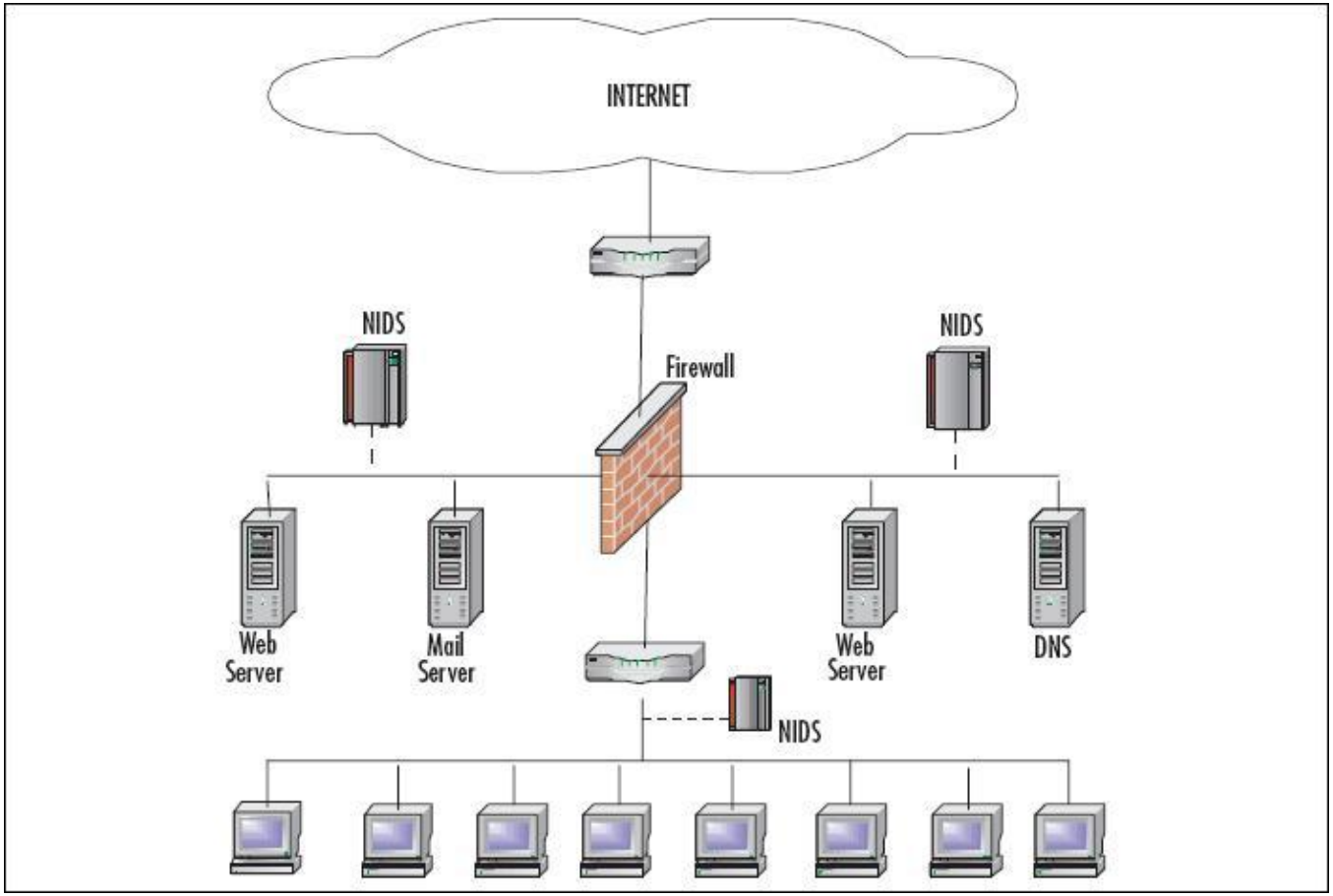
- possono ad es. bloccare una mail con un allegato eseguibile
- possono rilevare anomalie nell'utilizzo delle risorse del sistema, ad es. decine di mail spedite in breve tempo, grosse quantità di dati trasferiti, numero di connessioni aperte elevato, ecc… che possono permettere di individuare la presenza di un malware non riconosciuto dall'antivirus

Contromisure: IDS e IPS

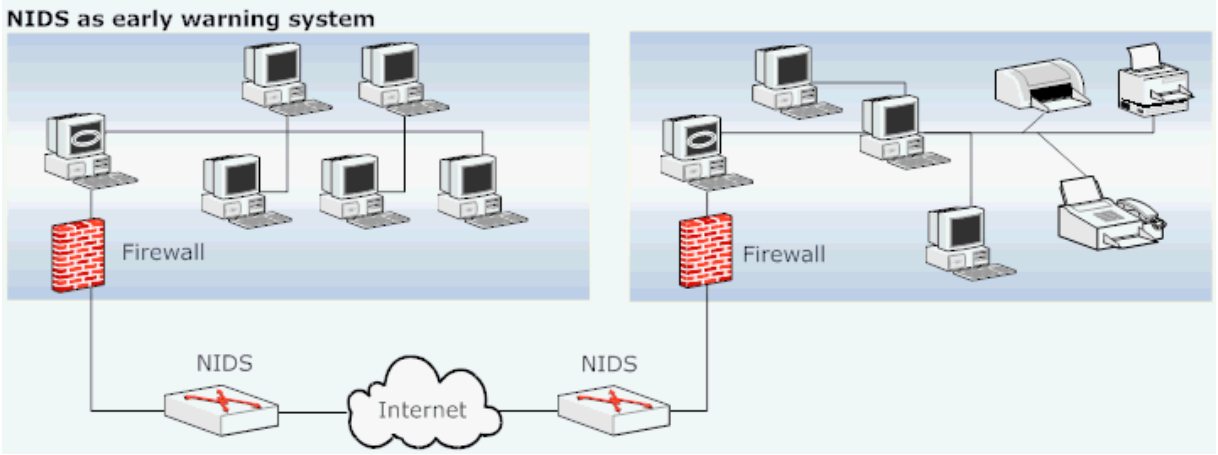
Gli IDS si distinguono in…

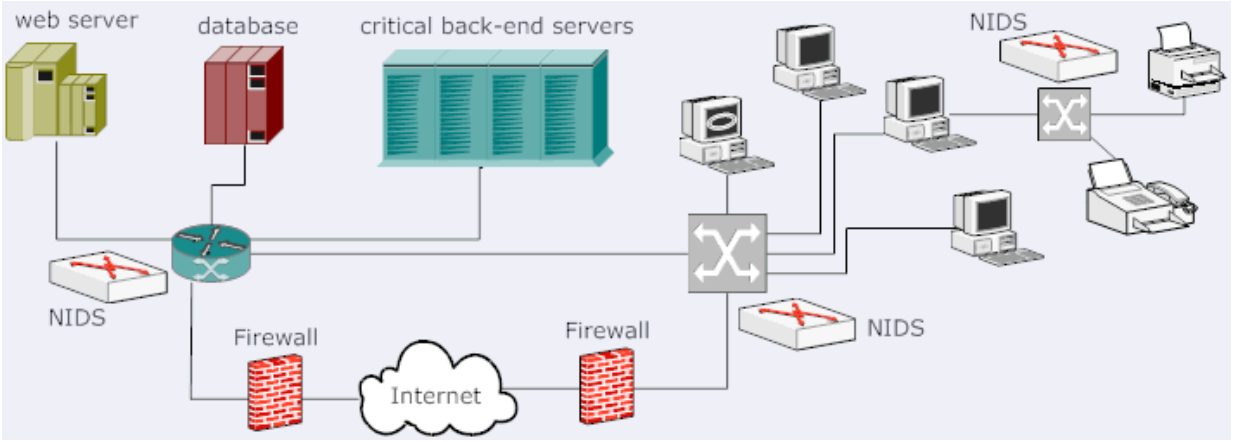
- HIDS(Host IDS) :
  - analizzano le attività dei singoli host, analizzando non solo il traffico di rete ma tutte le operazioni eseguite su quei sistemi (utenti – applicazioni – log) .
  - E' in grado di rilevare pertanto se un word-processor sta tentando di cambiare la password per l'accesso al database, può verificare che i file presenti sul computer non vengano alterati e che le attività svolte rientrino nella «norma»
- NIDS(Network IDS) : analizzano il traffico di rete alla ricerca di segnali di un attacco

NIDS

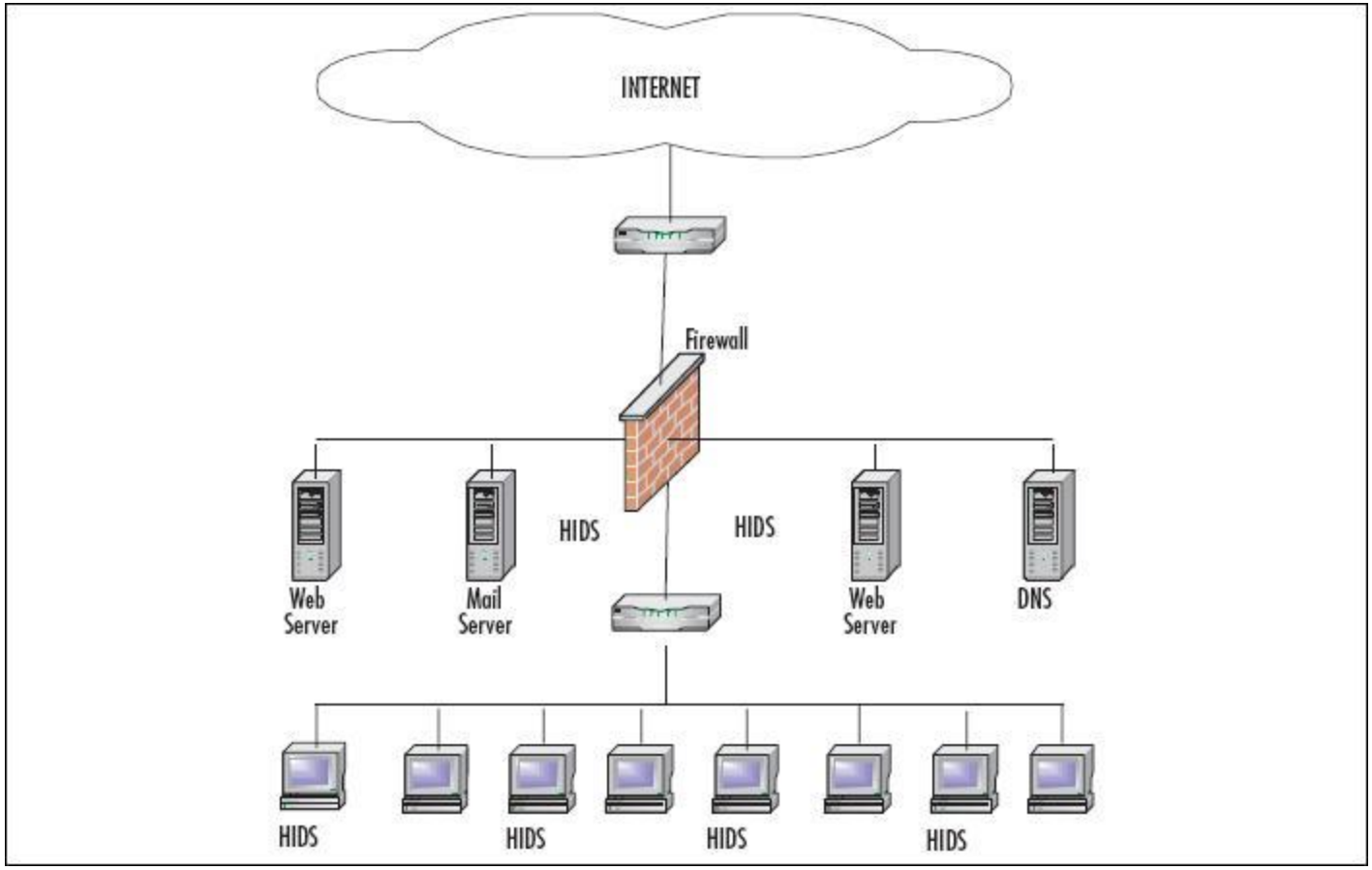

INTERNET
NIDS
Firewall
NIDS
Web Server
Mail Server
Web Server
DNS
NIDS

NIDS: collocazione





HIDS


INTERNET
Firewall
HIDS
HIDS
Web Server
Mail Server
Web Server
DNS
HIDS
HIDS
HIDS
HIDS

Backup

Creazione di copie dei dati.

Può essere :

- Locale: le copie sono conservate nello stesso luogo dove sono create
- Remoto: inviate attraverso internet a server remoti (previene da incendi, furti, ecc…)
- Parziale : riguarda solo parte dei dati
- Incrementale: vengono salvate solo le modifiche rispetto all'ultima versione(sono necessari tutti i file)
- Differenziale: vengono salvate tutte le modifiche rispetto all' «immagine completa»(sono necessari solo 2 file: l'immagine completa e quella differenziale)
- Crittografato

Formazione del personale

- La formazione del personale è forse la contromisura più efficace…
- Adottare costose soluzioni hardware o software e imporre rigorose politiche di sicurezza possono produrre un falso senso di sicurezza
- Tuttavia la non adeguata applicazione delle regole stabilite o l'ingegneria sociale possono rendere il sistema facilmente vulnerabile
- E' necessario capire quali informazioni sono importanti…e come comportarsi quando qualcuno le richiede…

Contromisure

Per approfondire

Lez-Jus-Info-07.pdf