LINUX DAY 2014 ITALIA

GULP

Giuseppe Augiero

FIREWALL (IN) SECURITY

Augiero.it

Linux Day 2014 - 25 ottobre 2014 - Mix Art

AGENDA

SICUREZZA INFORMATICA

- Introduzione

FIREWALL INSECURITY

- Possono creare falle nella sicurezza?

POSSIBILI ATTACCHI

- Analisi di attacchi di rete

ICT SECURITY

DEEP INSPECTION

- Per **sicurezza informatica** si intende quel ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce o attacchi e quindi della protezione dell'integrità fisica (hardware) e logico-funzionale (software) di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con un utente.
- Deve garantire:
    - la correttezza dei dati (integrità);
    - la confidenzialità dei dati (cifratura);
    - l'accesso fisico e/o logico solo ad utenti autorizzati (autenticazione);
    - la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (disponibilità);
    - la protezione del sistema da attacchi di software malevoli per garantire i precedenti requisiti.

ICT SECURITY

LA SICUREZZA

- Possiamo affermare:
  - **la sicurezza totale (100%) non esiste.**
  - **il concetto di sicurezza è prettamente soggettivo.**
  - **la sicurezza è un processo iterativo.**

ICT SECURITY

SVILUPPO

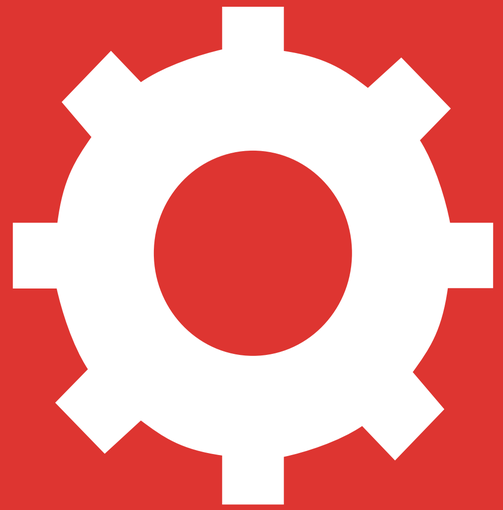
La sicurezza non ha uno sviluppo statico ma è un **processo iterativo**.

ICT SECURITY

COSTI

- ***I costi da sostenere sono inferiori al costo che l'organizzazione sosterrebbe in caso di compromissione del sistema.***

ANELLO DEBOLE

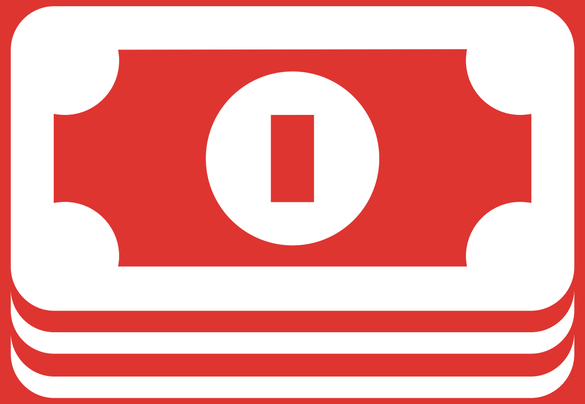


FIREWALL

FIREWALL

DIFESA

- Rappresenta la prima linea di difesa contro possibili attaccanti.
- Generalmente è posizionato sul perimetro tra la rete da proteggere e il resto del mondo (Internet).
- Isola un “pezzo di rete” offrendo ad essa una possibile soluzione di sicurezza.



IL VOSTRO FIREWALL È SICURO?

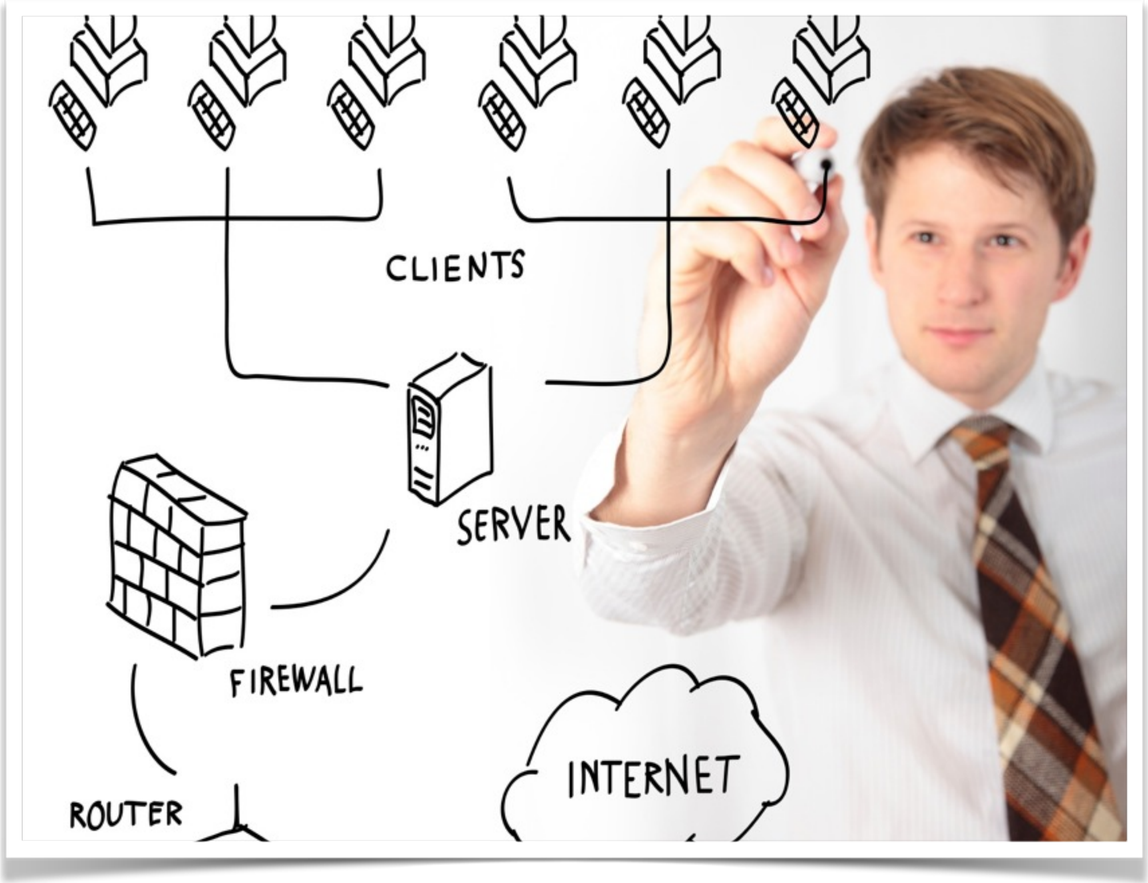
FULL SECURITY?

STRUMENTO COMPLESSO

- La semplice installazione e messa in produzione di un firewall non è sinonimo di sicurezza informatica.
- Il Firewall non può essere la panacea a tutti i mali.
- Non basta “installarlo”.

UN FIREWALL “MAL CONFIGURATO” O IL CUI DESIGN È ERRATO PORTA AD ABBASSARE IL LIVELLO DI SICUREZZA DELL’INTERNO SISTEMA.

DESIGN



IL NETWORK

- Il design del proprio network è stato realizzato in maniera corretta?
- Siamo sicuri che il firewall rappresenti l'unico punto di ingresso e uscita verso il "resto del mondo"?
- Potremmo non essere a conoscenza di ulteriori punti di contatto con altre reti (Es. Chiavette, routing errato, Wifi).

NAT

- IL NAT NON È SINONIMO DI SICUREZZA!!!

PERSONAL FIREWALL

SECURITY?

- Molto popolari e grande parco di software installato.

- Sono sempre efficaci?
- Ci proteggono sempre?

- Problema del Windows Network Architecture e del relativo LSP.
  - Bypass.
  - Analisi del traffico.

LE MINACCE

DA DOVE ARRIVANO?

- **Outsider** attack.
- **Insider** attack.

- Occorre non sottovalutare gli attacchi dall'interno della rete da proteggere.

- Meglio posizionare un secondo firewall prima del datacenter.

FIREWALL “SOFT”

“BASTIONIZZARE”

- Se il firewall utilizzato è una soluzione software occorre rendere sicura la macchina che lo ospita.
- Il server che fa girare il firewall non dovrebbe ospitare altri servizi.
- Il non corretto irrobustimento della macchina porta inevitabilmente a una possibile falla di sicurazza.
- Implicitamente la sicurezza dipende anche dal sistema operativo (patch, servizio ecc).

PACKET FILTER

FUNZIONAMENTO

- Un packet filtering firewall semplicemente esamina l'intestazione di ciascun pacchetto (IP) e decide se lasciarlo transitare o di bloccarlo in funzione delle regole definite dall'amministratore del firewall.

- Per definire una singola policy di sicurezza occorre definire una ennupla per "matchare" il traffico desiderato:
    - Source Ip
    - Destination IP
    - Protocol
    - source / destination port

PACKET FILTER

INSECURITY

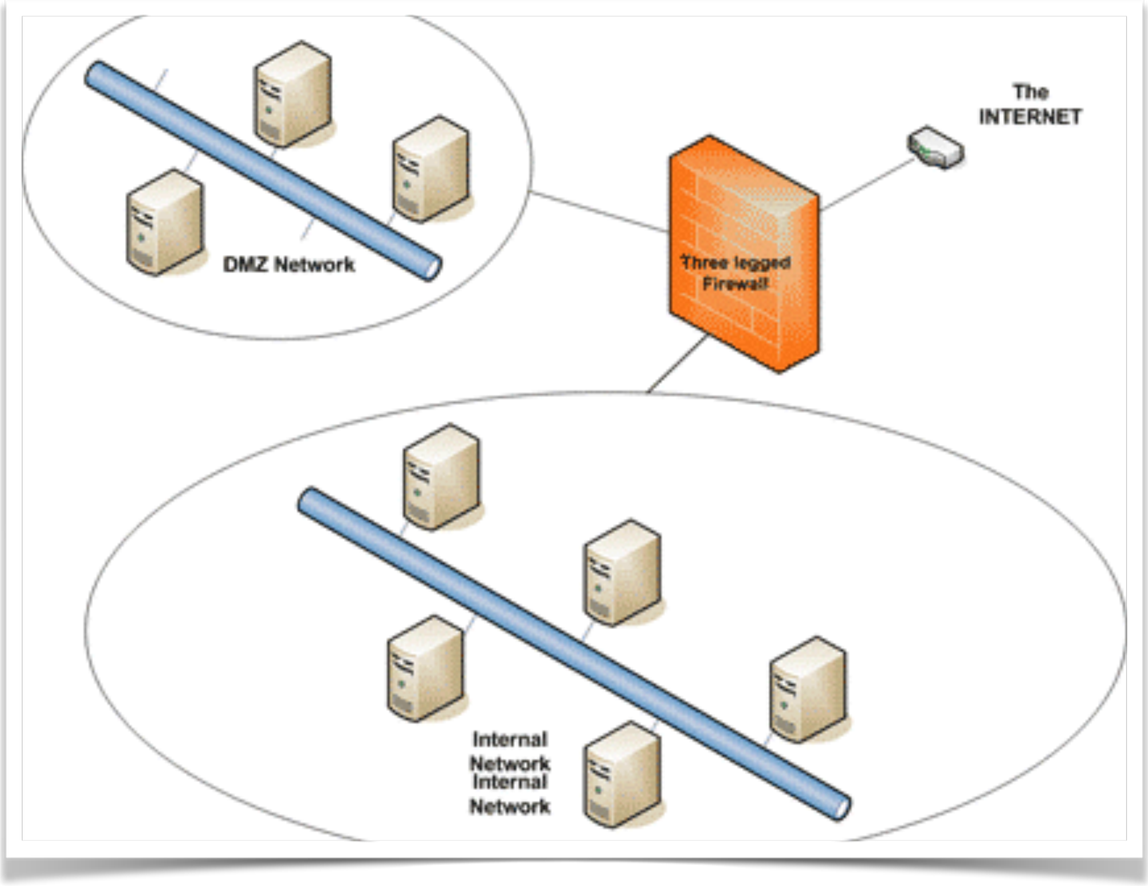
- I firewall basati su packet filter nascono oltre 20 anni fa e ormai non rappresentano una scelta sufficiente per filtrare il traffico di rete.
- Riconoscere e filtrare il traffico lavorando solo sui livelli sottostanti a quello applicativo non permette di avere la giusta granularità.
- Soluzione molto economica usata soprattutto in ambito soho.
- Prodotto incompleto per le attuali esigenze di sicurezza.

STATEFULL INSPECTION

INSECURITY

- Passare allo statefull inspection, mantenendo informazioni sullo stato delle connessioni, è utile ma non ci garantisce, sino in fondo, quello che vorremmo.
- Il grado di sicurezza non aumenta in maniera decisiva.
- E’ sicuramente da preferire al semplice packet filter.
- Anche questa soluzione non è sufficiente, da sola, a garantire un buon grado di sicurezza.

DMZ



SERVIZI IN PRODUZIONE

- Per offrire servizi esterni non basta creare e gestire una DMZ.
- L'implementazione di private vlan e di meccanismi di separazione e confinamento è necessaria per garantire una maggiore sicurezza.

SECURITY POLICY

LE REGOLE DEL GIOCO

- Definire policy di sicurezza potrebbe non essere facile e può indurre ad errori.

- Security breach potrebbero derivare da:
    - policy scritte in maniera errata.
    - policy temporanee dimenticate.
    - errato ordine delle regole.
    - deroghe mal definite.
    - policy inesistenti.

FALSI POSITIVI - VERI

CREARE CONFUSIONE

- Attenzione nel rimuovere regole che sembrano generare solo falsi positivi.

- E’ possibile creare un attacco ad hoc con fine di far eliminare o modificare una buona policy presente nel firewall.

- Tre step:
  - Continui falsi positivi.
  - Rimozione policy.
  - Attacco vero e proprio.

LIVELLO APPLICATIVO

HTTP

- Ormai buona parte del traffico verso Internet è uno stream http.
- Una semplice regola di un packet filter che permette il passaggio del traffico verso la porta 80 di un nostro webserver potrebbe permettere un sql-injection.
- E’ impossibile discriminare il traffico in uscita.
- Content Delivery Network.

LIVELLO APPLICATIVO

FIREWALL L7

- Occorre necessariamente fare analisi a livello applicativo.
- E' possibile, in questo modo, discriminare per singolo stream http e quindi per singola applicazione (Gmail, Facebook, Skype, DropBox).
- Può essere utile usare anche tecniche statistiche.
- In alcuni casi è l'unico modo per filtrare o bloccare alcune applicazioni (ad es.TeamViewer).

LIVELLO APPLICATIVO

DEEP INSPECTION

- Un pacchetto che venga riconosciuto aderente ai criteri prestabiliti può essere gestito dai dispositivi DPI in varie forme, tra cui scartato, rediretto, variata la sua priorità, ne puo' essere limitato il bit rate (la "velocità" massima di questo flusso di pacchetti e anche notificato a un sistema di monitoraggio).

- **La Deep Inspection va usata cum grano salis.**

FIREWALL EVASION

EAT

- Tecniche più o meno avanzate per bypassare il firewall.

- Comune denominatore:
  - spezzettamento del payload malevole in pezzettini più piccoli.
  - camuffamento.
  - trasporto del payload frazionato con più protocolli.
  - riassemblaggio.

I CATTIVI SONO FUORI

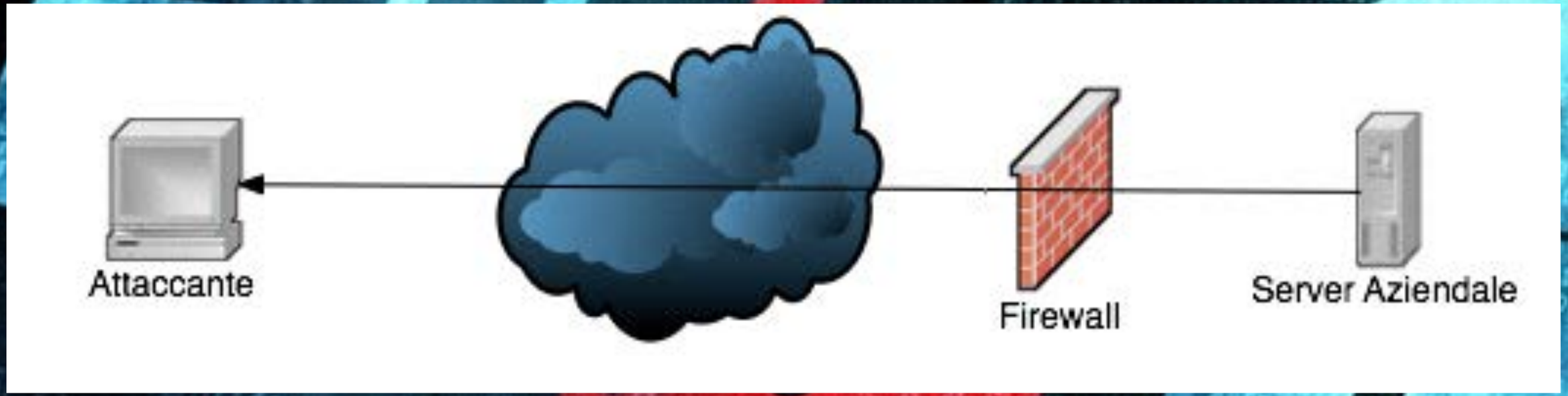
ONE WAY

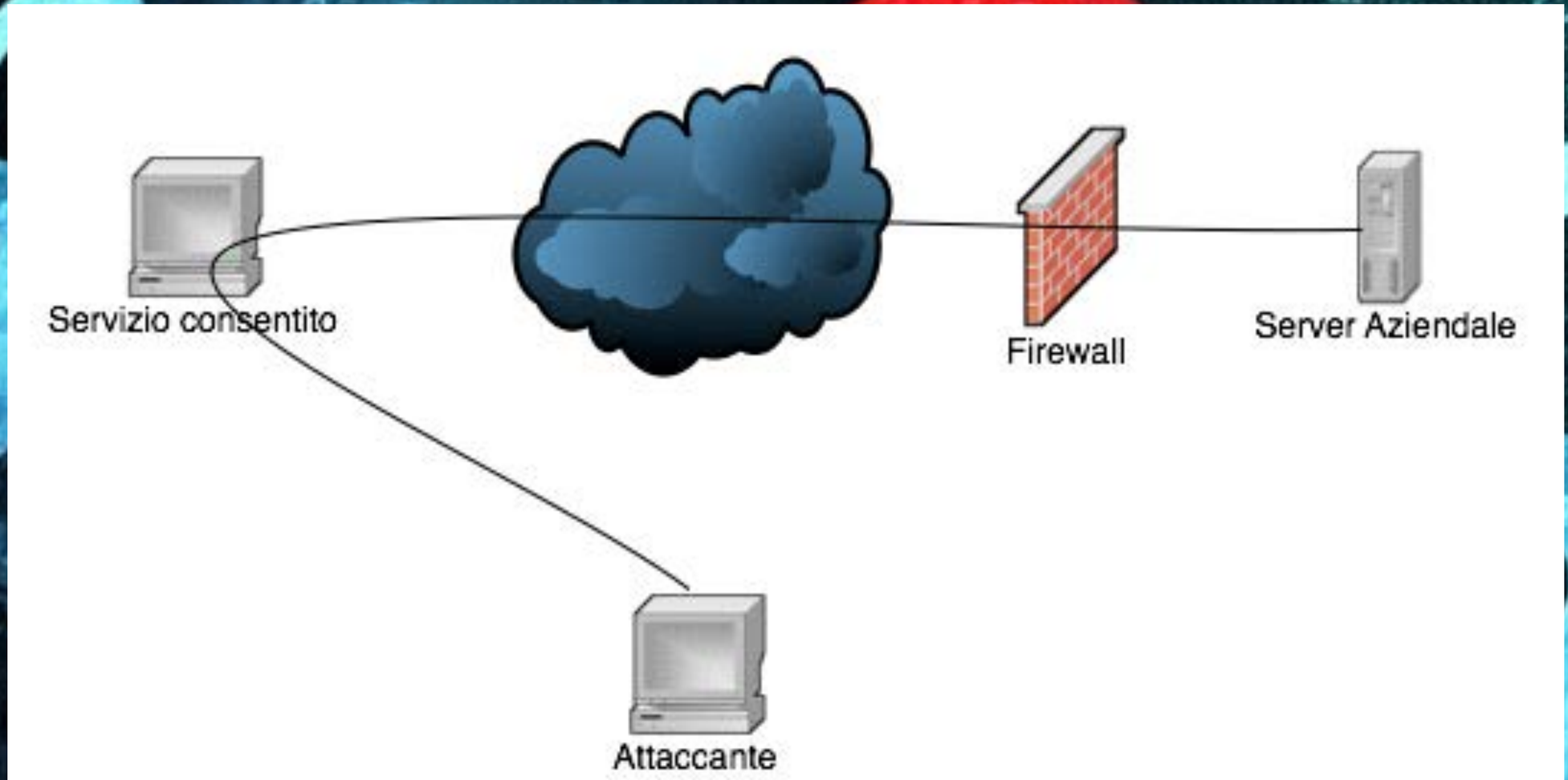
- Molti firewall vengono configurati in modo da filtrare in maniera puntuale il traffico dall'esterno verso l'interno mentre lasciano passare tutto o quasi tutto nel senso opposto.

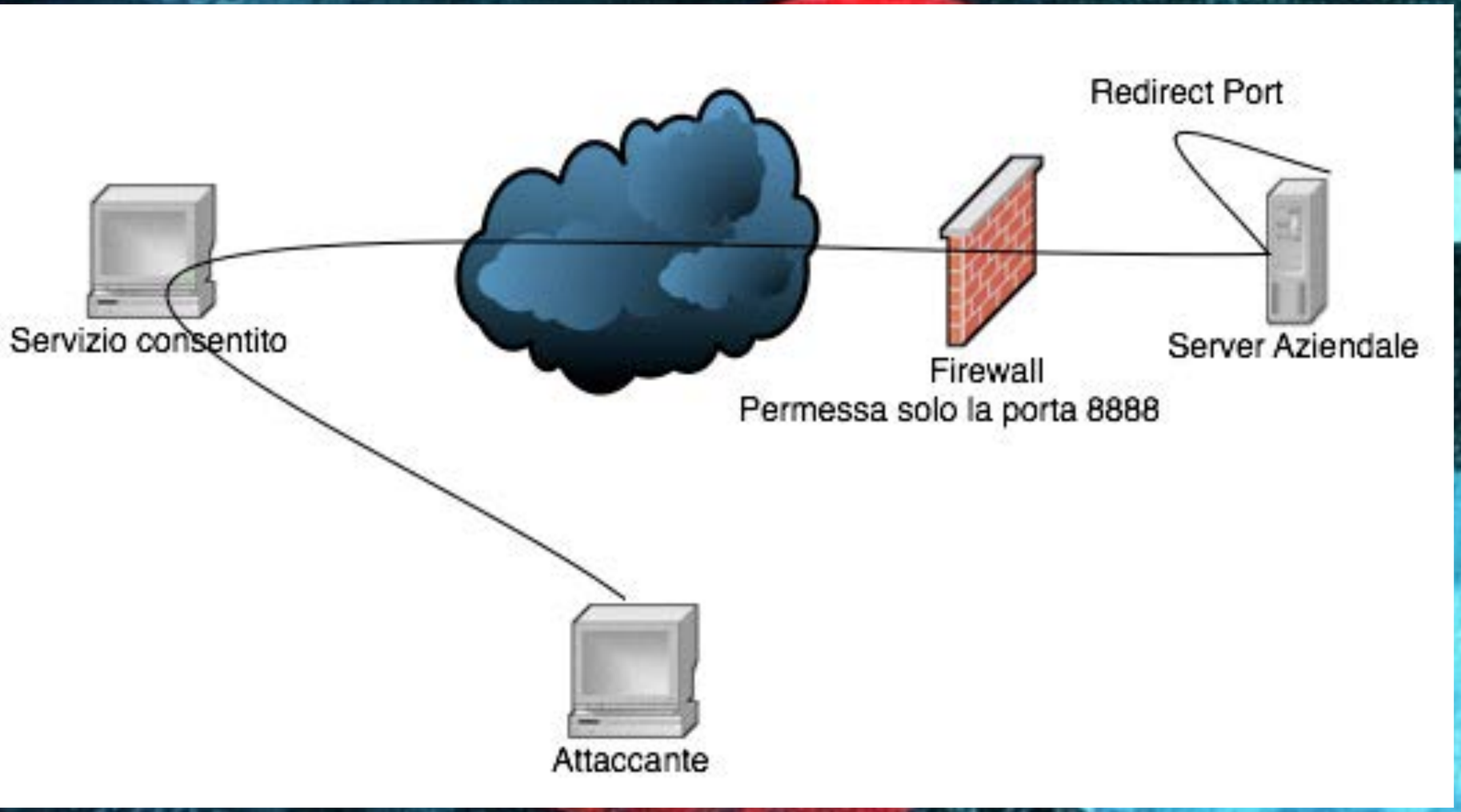
- Cosa succede se l'attaccante esterno riesce ad aprire una connessione verso di lui che nasce dall'interno?

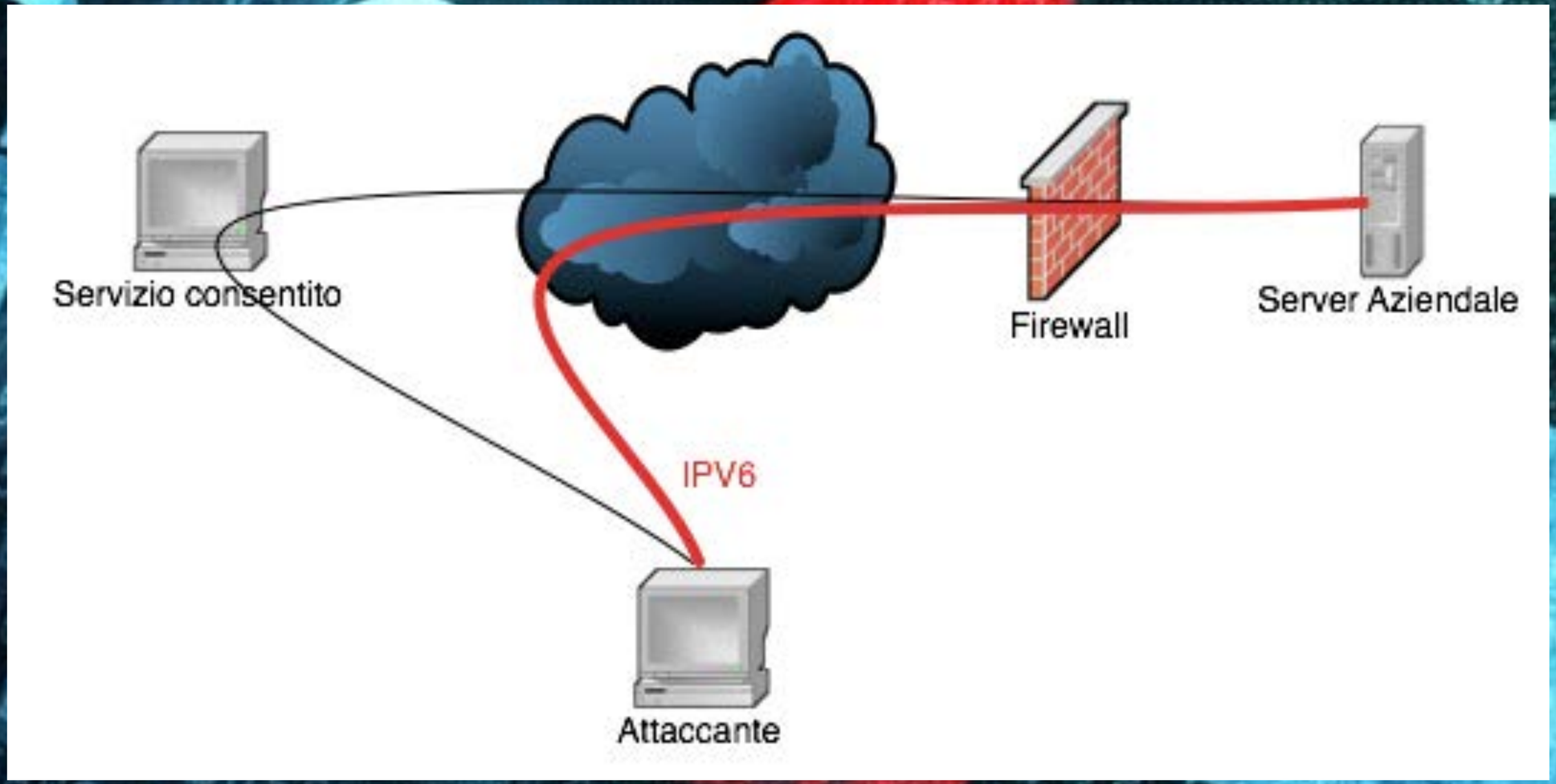
- Macchine infette e Zombie.

POSSIBILI ATTACCHI


Attaccante
Firewall
Server Aziendale


Servizio consentito
Firewall
Server Aziendale
Attaccante


Redirect Port
Servizio consentito
Firewall
Permessa solo la porta 8888
Server Aziendale
Attaccante


Servizio consentito
IPV6
Attaccante
Firewall
Server Aziendale

CONCLUSIONI

FIREWALL???

QUALE STRADA INTRAPRENDERE?

- Occorre cambiare radicalmente l'approccio nella definizione delle policy di sicurezza.
- Necessità di continui audit e tunning al proprio sistema di sicurezza.
- Cooperazione tra più soluzioni eterogenee.
- Analisi delle anomalie attraverso l'analisi dei flussi di rete.
- Concatenazione degli eventi (firewall, ids, …).

GRAZIE !!!

CONTATTI:

EMAIL: TALK@AUGIERO.IT

TWITTER: @GIUSEPPEAUGIERO

WWW.AUGIERO.IT

LINUX DAY 2014 ITALIA

GULP

Giuseppe Augiero

FIREWALL (IN) SECURITY

Augiero.it

Linux Day 2014 - 25 ottobre 2014 - Mix Art