Come mettere in sicurezza i sistemi informatici di una PA

VINCENZO CALABRÒ

AGENDA

Agenda

Sicurezza di rete

- Minacce
- Cosa ci interessa
- Sicurezza e analisi del rischio
- Topologia e segmentazione
- Router utente/firewall il primo «scoglio»
  - Hardening router di bordo
  - Filtri antispoofing
- Come ruotare le reti pubbliche - DMZ (ACL sul router di bordo)

Agenda

- Come ruotare le reti interne (intranet, workstation) - Filtri su firewall interno
  - Policy per assegnazione di indirizzi (DHCP)
  - NAT
- Altri elementi infrastrutturali di rete
  - DNS
  - Sistema di autenticazione
  - LOG server
  - Monitoraggio di rete
- Aggiunta di ulteriori servizi: dove metterli e come ruotarli
  - wireless & BYOD
  - VPN
  - Stampanti, dispositivi IoT

Agenda

Sicurezza host (cenni)

- Minacce
- hardening linux
- hardening Windows
- Hardening di servizi (cenni): https, ssh

minacce

- Attacchi DoS e DDoS
- Virus/Malware
- Phishing
- BotNet
- Compromissione/estromissione dati sensibili
- Dispositivi IoT, stampanti, videosorveglianza
- Telefonini, tablet, PC personali, BYOD
- Far utilizzare la nostra rete per scopi non istituzionali

Cosa ci interessa

Legalmente e istituzionalmente (e umanamente):

- Ottemperare alle leggi come il GDPR e le misure minime di sicurezza
- Preservare la privacy delle persone e la riservatezza dei dati che trattiamo
- Offrire e garantire un certo livello di servizio agli utenti

AUP (Access User Policy)

- Ogni accesso alla rete deve essere nominativo
  (non possiamo dare accesso anonimo alla rete)
- Evitare che le nostre macchine creino problemi a terzi

Minimo sforzo e minima spesa per ottenere un risultato per noi accettabile

- Cosa significa «minimo sforzo» e «minima spesa»
  - Risparmio su risorse umane
  - Risparmio su hardware
  - Risparmio su software
- Come definire cio' che per noi e' accettabile
  - Stabilire cosa e' di vitale importanza e cosa puo' rompersi senza grossi problemi
  - Preferire meno hardware ma piu' intervento umano
  - Favorire l'automazione a causa di carenza di personale

Definizione degli scopi

Partiamo da definire quello che vogliamo fare

- Compiti istituzionali
- Servizi per utenti esterni
- Servizi per utenti interni e gestionali
- Servizi infrastrutturali, monitoraggio, audit

Chi parla con chi (e chi NO!)

Per ogni servizio offerto vanno valutate le relazioni e le connessioni fra di se' e con l'utenza

- il tipo di utenza che accede a quel servizio
- ruoli e privilegi (profilatura delle utenze)
- accessi di tipo macchina-macchina (web al DB)
- accessi di monitoraggio e gestione

Di quel che c'e'…

Non manca niente!

Facciamo il censimento di quello che abbiamo

- Hardware
- Software
- Infrastruttura di rete
- Persone!
- Risorse economiche

Risultato

- Dato quello che si vuole fare
- Stabilito chi fa cosa
- Censito quello che c'e'

Possiamo crearci uno schema di rete in modo da isolare il piu' possibile il tipo di utenze con i servizi di cui avranno bisogno

Ognuno potra' usare solo la sua bolla isolata

In termini «moderni»

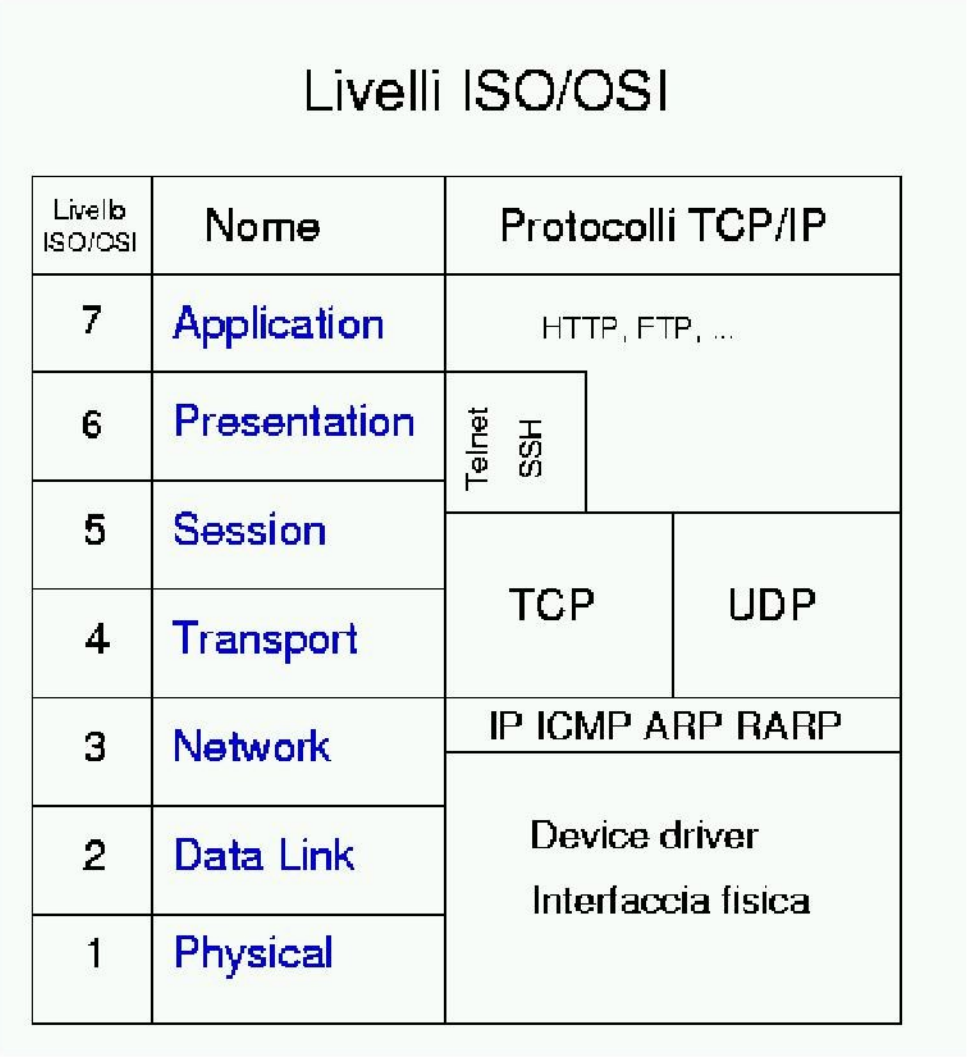
Nel gergo moderno (e pomposo) la slide di prima viene tradotta in:

- Stabilire gli ambiti e gli scopi
- Stabilire lo SLA (Service Level Agreement)
- Valutare l'assestment
- Effettuare l'analisi del rischio

Misure minime di sicurezza

- INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI
- INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
- PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
- VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
- USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
- DIFESE CONTRO I MALWARE
- COPIE DI SICUREZZA
- PROTEZIONE DEI DATI

Pila ISO/OSI


Livelli ISO/OSI
Livello ISO/OSI
Nome
Protocolli TCP/IP
7
Application
HTTP, FTP, ...
6
Presentation
Telnet
SSH
5
Session
4
Transport
TCP
UDP
3
Network
IP ICMP ARP RARP
2
Data Link
Device driver
Interfaccia fisica
1
Physical

Un po' di teoria

Protocollo IP: Protocollo di indirizzamento e instradamento fra reti

- Assegnazione di un indirizzo univoco
- Assegnazione percorso per raggiungere le reti
  - Rete locale tramite protocolli sottostanti
  - Rete esterna tramite la richiesta di instradamento al gateway

Classi di IP - Reti locali e Domini di Broadcast

- Classe A 10.0.0.0/8
- Classe B 10.1.0.0/16
- Classe C 10.2.2.0/24

Cenni di Routing

Istradamento a livello rete (3)

I router usano tabelle di instradamento i cui elementi sono blocchi di indirizzi IP contigui, che sono detti rotte

- **reti direttamente connesse**: quando una interfaccia di rete di un host viene configurata con un indirizzo IP ed una maschera di sottorete, l'host conosce automaticamente la rotta per raggiungere tutti gli host di quella sottorete.
- **statico**: le rotte possono essere configurate manualmente sul router che ha una interfaccia per ogni rete che instrada
- **routing dinamico**: le tabelle di instradamento vengono popolate da appositi protocolli di routing, implementati solitamente solo sui router fra router

Reti private

10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/16

Per convenzione non possono essere ruotate dall'esterno, serve un servizio che traduca gli indirizzi privati in indirizzi pubblici

NAT (Network Address Translation)

- Utile per segmentare la rete a piacimento
- Introdurre regole di accesso specifiche per ogni rete

Assegnazione automatica IP

Per configurare automaticamente un dispositivo da connettere alla rete si utilizza un servizio che per ogni client che fa richiesta, assegna un indirizzo IP (oltre alla subnet mask e default gw)

DHCP

Dinamico: il server DHCP assegna il primo indirizzo disponibile fra un pool preconfigurato

Statico: Ogni dispositivo ottiene SEMPRE un indirizzo associato al proprio MAC address

Sicurezza

All'interno di una sottorete il traffico passa

- Nessun controllo
- Nessuna regola possibile
- Possibile sniffing del traffico di altre macchine

Fra sottoreti eterogenee il traffico deve passare da un router/firewall

- Controllo su tutto il traffico fra reti eterogenee
- Possibilita' di stabilire regole e filtri
- Impossibilita' di sniffing

Strategia

Di importanza strategica per la sicurezza

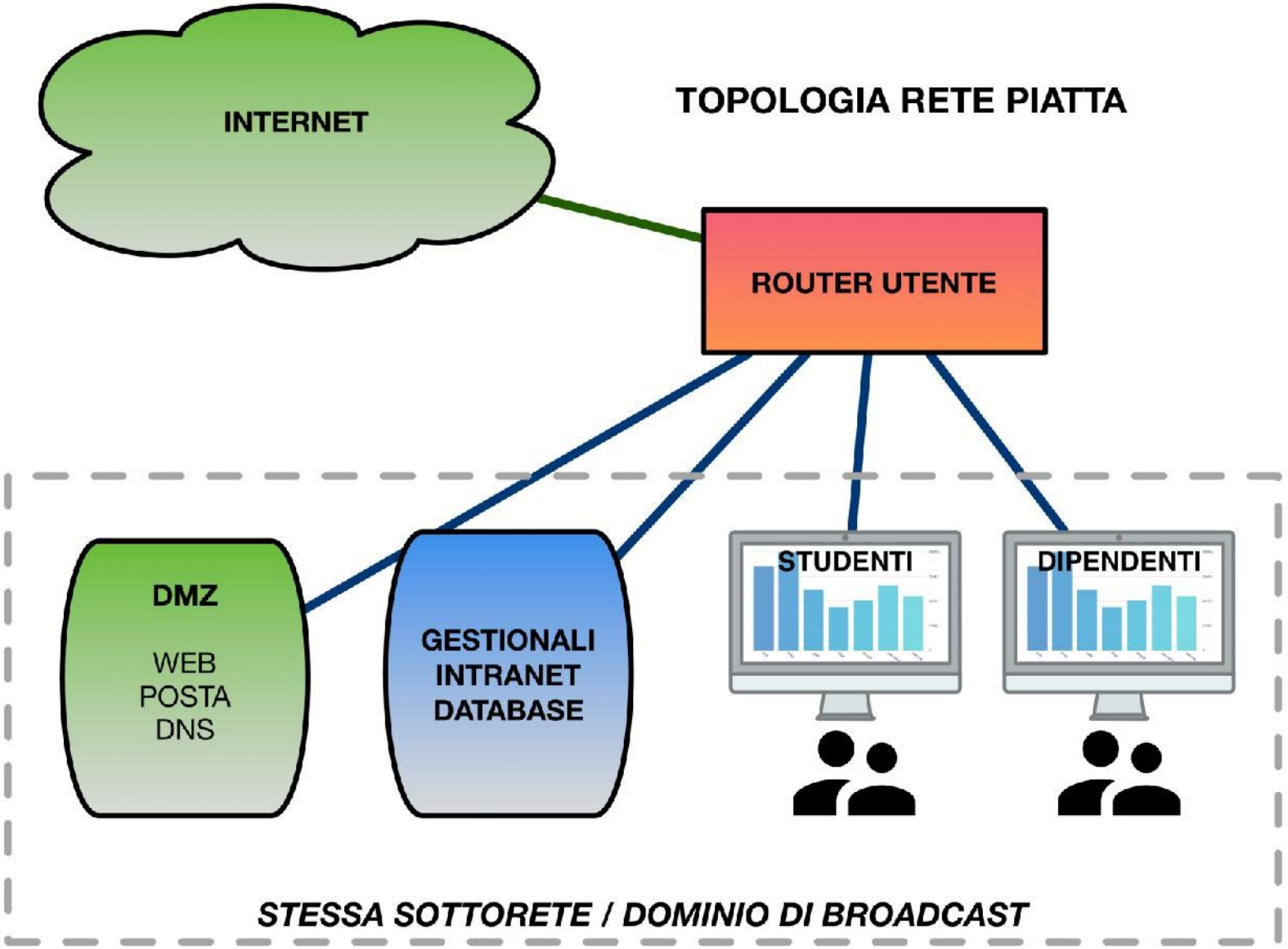
- Segmentazione della rete
- Regole specifiche di ingresso e uscita per ciascuna rete (o segmento o servizio)
- Assegnazione statica di indirizzi IP, quindi assegnazione della rete di appartenenza, con le proprie regole gia' stabilite

Punti importanti

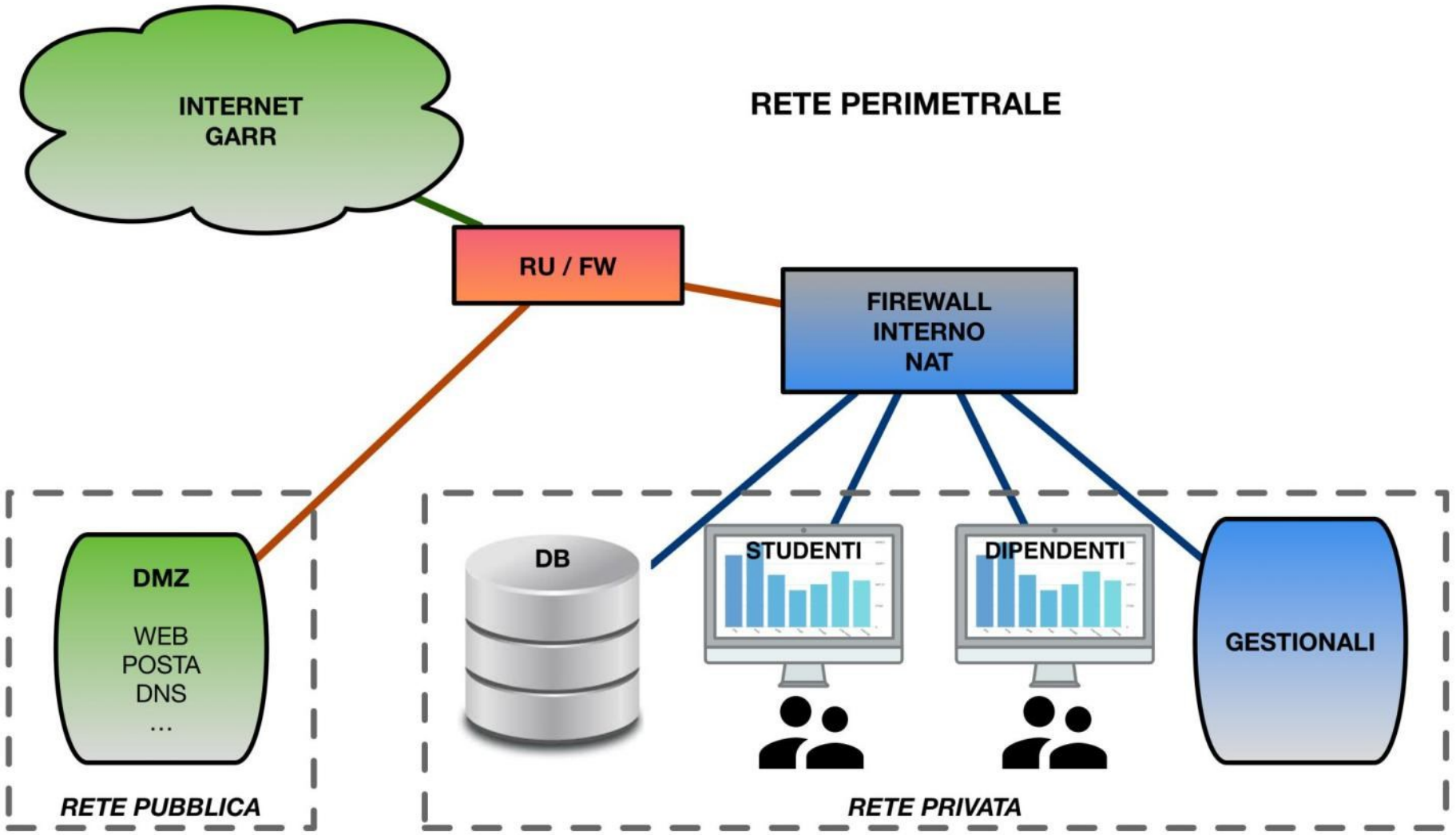
- Bloccare tutto meno lo stretto necessario
- Permettere l'accesso a un certo segmento di rete (servizio) solo a chi ne ha diritto
- Assegnare indirizzi e reti appropriate all'utilizzo del dispositivo
- Registrare i MAC Address sul DHCP per evitare accessi anonimi e/o installazione di HUB
- Solo accessi autenticati negli altri casi

SEGMENTARE IS DA WEY

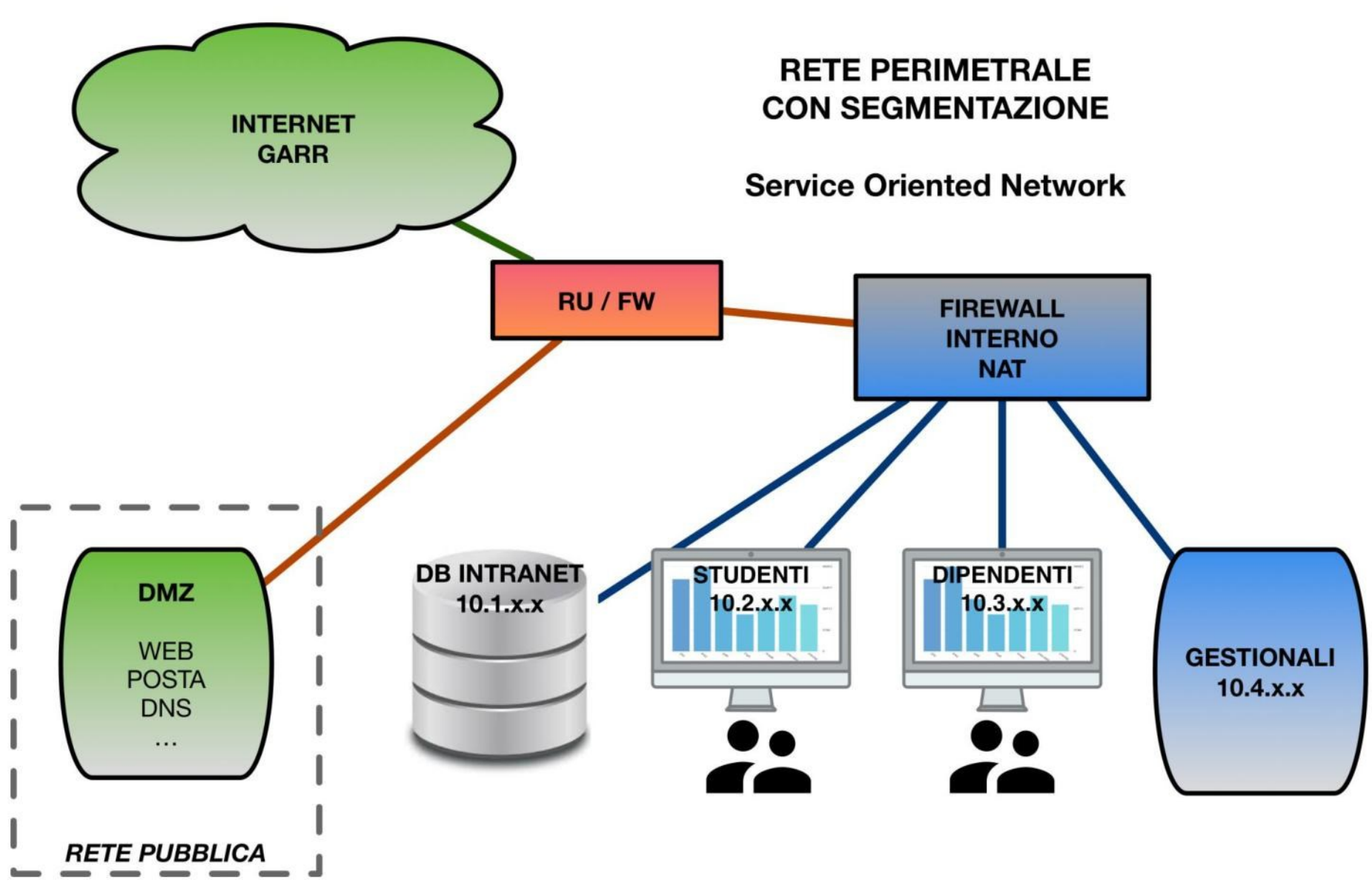
Topologia FLAT



Topologia perimetrale



Perimetrale segmentata



Perimetrale

E’ composta da una parte di rete pubblica dove stanno tutti e soltanto i servizi accessibili ad utenti esterni, detta DMZ

- Sito web istituzionale
- Server di posta (o relay o mail gateway)
- Server DNS autoritativo per il proprio dominio
- Firewall verso rete interna
- Eventuale VPN, wi-fi etc etc

E una parte intranet non accessibile dall’esterno

- Gestionali
- PC workstation
- DB… Etc etc

IL ROUTER

Router di bordo

E’ il router che ha l’unica interfaccia che ci connette verso internet

E’ il portone d’ingresso e di uscita di ogni pacchetto della nostra rete:

deve essere messo in sicurezza lui per primo

Router di accesso

Il router di bordo e' inoltre il primo scoglio dove si scontra chiunque provenga dall'esterno.

E' necessario configurare in questo punto

- Filtri antispoofing
- Regole di accesso: cosa instradare e dove
  - ACL generali in entrata/uscita
  - ACL verso la DMZ

Stateful o Stateless

I router si dividono in due grandi famiglie

Sateless:

- Elaborano un pacchetto per volta, applicano le regole di filtering/firewalling e passano al pacchetto successivo
- Non tengono memoria delle connessioni o delle sessioni
- Hanno default policy di filtering tutto permit

Stateful:

- Fanno deep inspection del pacchetto
- Riescono a capire se un gruppo di pacchetti fa parte della stessa sessione
- Tengono una tabella in memoria con le sessioni
- Hanno default policy di filtering a reject

Configurazioni SF SL

I router stateless sono quelli di prima generazione, piu' antichi. Perlopiu' tutti i router moderni sono stateful

Oltre alla differenza di prezzo lo stateful garantisce maggior sicurezza ma minor prestazioni dato che deve ispezionare il pacchetto

La grossa differenza e' in fase di configurazione:

- Stateful: default policy DENY ALL

  E si aggiungono le poche permit che servono
- Stateless: default policy ALLOW ALL

  Vanno aggiunte righe per togliere tutto quello che non ci serve

Hardening router

- Togliere l'accesso via telnet: non siamo negli anni '90, nessuno usa piu' telnet!!
- Abilitare e configurare l'accesso ssh
- Creare utenti e gruppi
- Togliere possibilmente l'accesso web
- Valutare soltanto uno o pochissimi IP che possono accedere via ssh e/o web
- Configurare un log server remoto
- Tenere il sistema operativo all'ultima versione

Esempio: Cisco router

Disabilito telnet e accendo ssh:

```
line vty 0 15
access-class 100 in (possono accedere solo gli host in access-list 100)
transport input ssh
ip domain-name <tuo.dominio>
ip ssh version 2
crypto key generate rsa
service password-encryption
```

Definisco la "enable password" o un utente privilegiato:

```
enable secret/password la-tua-enable-password  (dipende dal modello)
username <nome utente> privilege level 15 password <password>
username nocview privilege level 7 password *******
```

Creo una access-list per l'interfaccia web (HTTPS) e l'abilito:

```
ip http secure-server
no ip http server
ip http access-class 20 (possono accedere soltanto gli host in access-list 20)
```

Configuro un log server remoto:

```
service timestamps log datetime
!definisce il nome del file che contiene i log
logging trap debugging <NOME LOG FILE>
!definisce l'IP del syslog server
logging facility logging <IP LOG SERVER>
```

Esempio: Juniper router (1/4)

Disabilito telnet e abilito ssh:

```
delete system services telnet
services {
    ssh {
        protocol-version v2;
    }
```

Definisco un utente privilegiato:

```
class tier3 {
idle-timeout 15;
/* Fornisce un accesso illimitato */
permissions all;
  }
/* Account root locale con password locale */
        user admin {
            full-name Administrator;
            uid 2000;
            class tier3;
            authentication {
                encrypted-password "<PASSWORD>"; # SECRET-DATA
            }
```

Juniper router (2/4)

Definisco l'accesso (sola lettura):

```
class tier1 {
/* La sessione va in time out dopo 15 min di inattivita' */
      idle-timeout 15;
      /* Fornisce privilegi di sola lettura*/
permissions [ configure interface network routing snmp system
class tier1 {
/* La sessione va in time out dopo 15 min di inattivita' */
      idle-timeout 15;
      /* Fornisce privilegi di sola lettura*/
permissions [ configure interface network routing snmp system
 trace view firewall ];
/* Account nocview locale con password locale */
        user nocview {
            uid 2001;
            class tier1;
            authentication {
                encrypted-password "*******"; # SECRET-DATA
              }
       }}
```

Juniper router (3/4)

Restringo l'accesso all'interfaccia web:

```
policy-options { prefix-list trusted-ips { 111.xxx.xxx.xxx/32; }
}
firewall {
    filter trusted-ips {
        term block_non_trusted {
            from {
                source-address {
                    0.0.0.0/0;
                }
                source-prefix-list {
                    trusted-ips except;
                }
                protocol tcp;
                destination-port [ https ];
            }
            then {
                discard;
            }
        }
        term accept_all {
            then accept;
        }
    }}
```

Juniper router (4/4)

Definire syslog remoto:

```
syslog {
        /* Archivia i vecchi file fino a 10M */
        archive size 1m files 10;
        user * {
            any emergency;
        }
        /* Invia i log data verso il syslog server */
        host <IP LOG SERVER> {
            any info;
        }
        file messages {
            any notice;
            authorization info;
        }
    }
```

Filtri antispoofing

Lo spoofing e' una tecnica largamente ultilizzata per effettuare attacchi di tipo DoS o DDoS

Consiste nella creazione di un pacchetto IP nel quale viene falsificato l'indirizzo IP del mittente (la vittima designata del DDoS). In questo caso abbiamo routing asimmetrico perché un eventuale pacchetto di risposta viene inviato al vero IP, che sara' subissato e morira'

Il router in sicurezza deve ruotare soltanto pacchetti che abbiano la propria rete come sorgente o destinazione, non devono ruotare pacchetti con IP sorgenti le vittime dei DoS

Non e' nostra competenza per esempio ruotare un pacchetto che da repubblica.it va a google - dobbiamo scartarlo

Esempio

Supponiamo che sono dentro l'universita' di Topolinia (192.84.145.0/24) e che voglia affossare la macchina 1.1.1.1

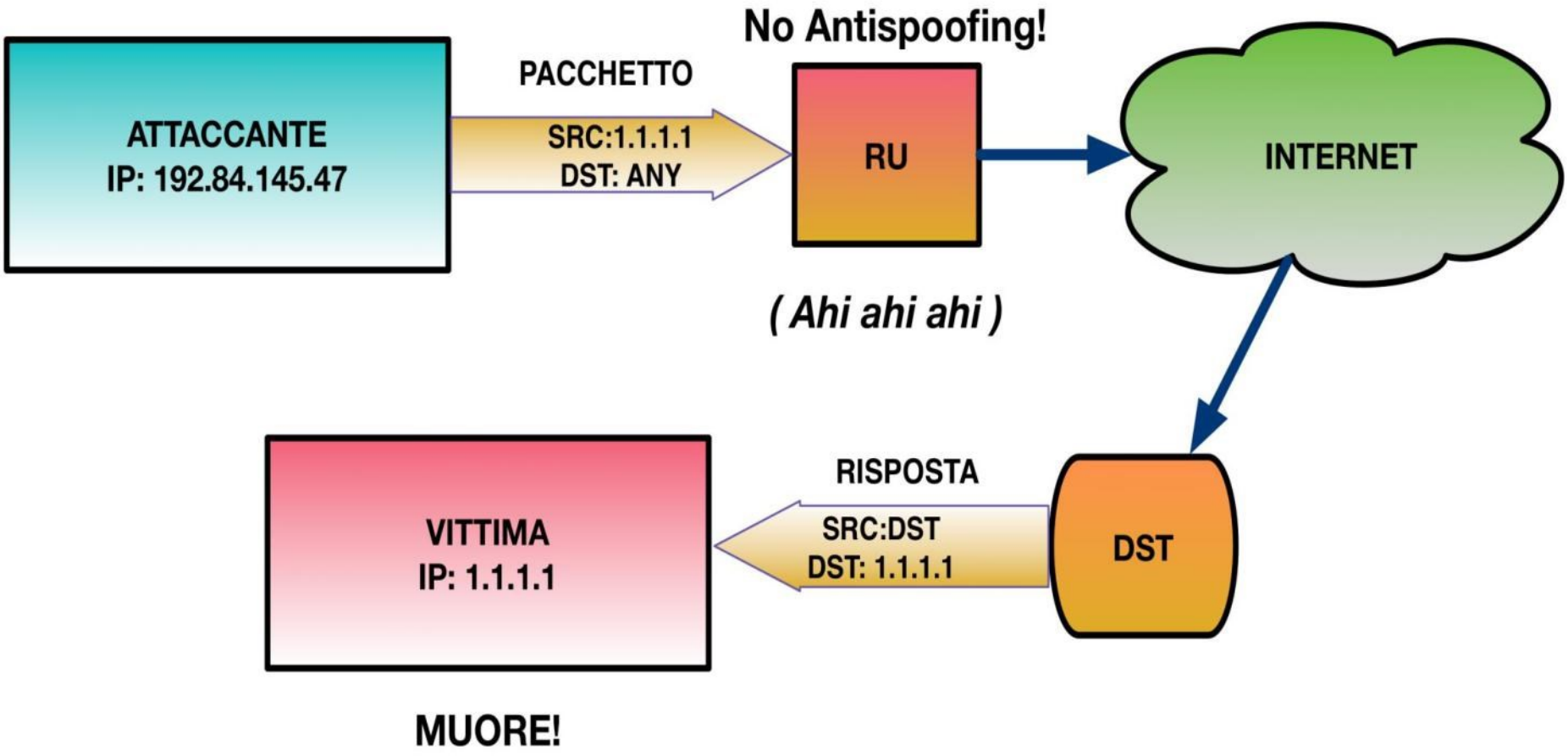
Dalla mia macchina (192.84.145.250) mando un treno di pacchetti falsificati con

SRC: 1.1.1.1, DST qualsiasi

Senza filtro antispoofing: qualsiasi macchina DST risponderebbe e il messaggio di risposta andrebbe alla sorgente, 1.1.1.1 che risulta DoSsata

Col filtro antispoofing: il router di bordo si accorgerebbe che sta venendo dalla rete interna verso la rete esterna un treno di pacchetti che non e' di sua competenza, e lo scarterebbe, evitanto il DoS

Graficamente



Regole antispoofing

Cisco router:

```
access-list 115 remark Anti-spoofing ACL
access-list 115 permit ip 192.84.145.0 0.0.0.255 any
access-list 115 deny ip any any log-input
```

Regole antispoofing

Juniper router:

```
filter outbound-filter {
        term 1 {
            from {
source-address {
                    192.84.145.0/24;
                     }
            }
            then accept;
        }
        term 2 {
            then {
                count spoof-outbound;
                discard;
            }
        }
    }
```

IL FILTERING IN DMZ

ACL di protezione

Regole per utenti che provengono dall'esterno o guest

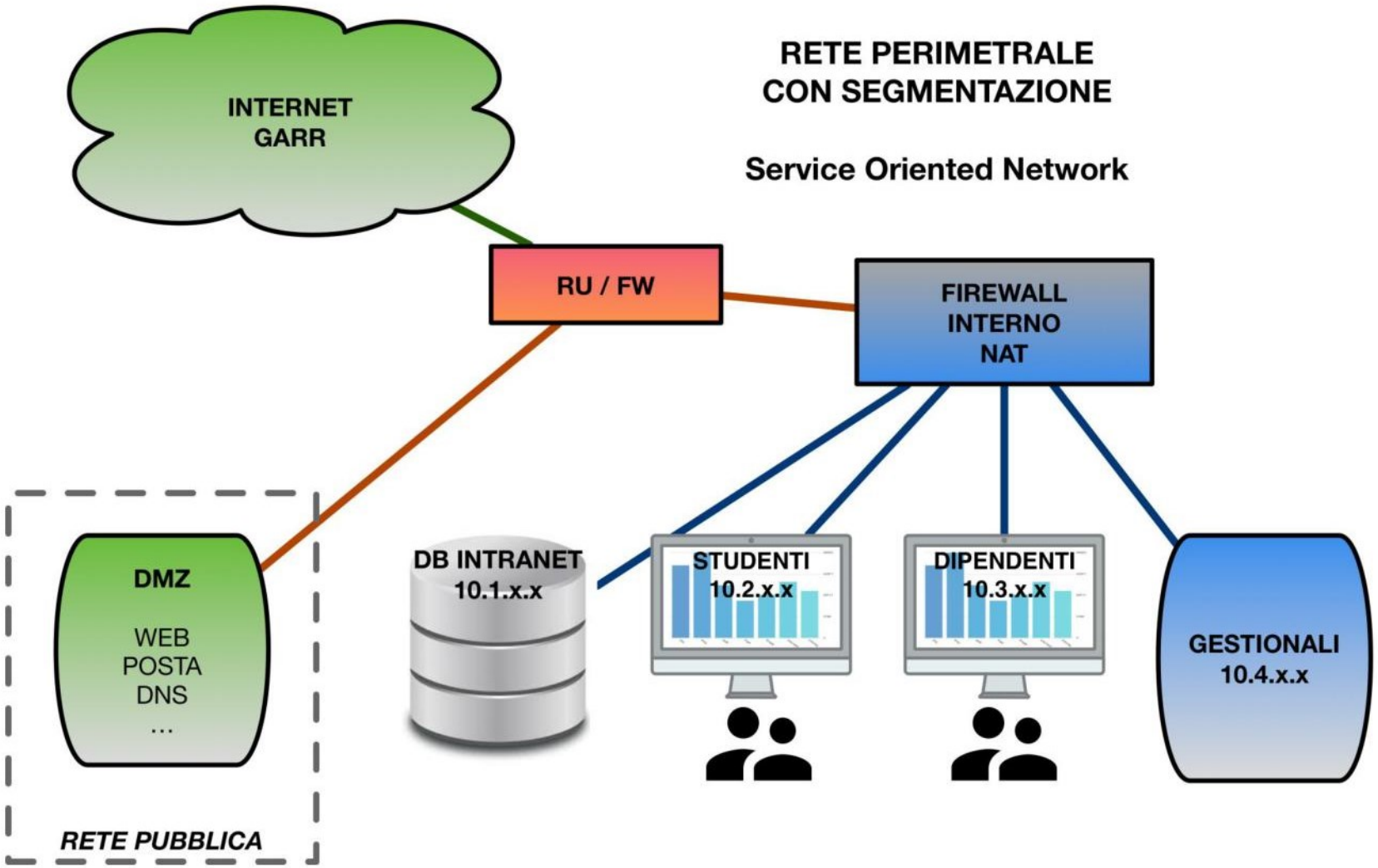
Blocco tutto di default e apertura soltanto verso servizi in DMZ

- web
- Posta
- DNS
- eventuale VPN, wi-fi etc etc

ACL - Filosofia

- Blocchiamo tutto tranne le cose che servono:
- Traffico in ingresso «ETABLISHED»
- Traffico DNS sul server DNS
- Traffico web (HTTP/HTTPS) sul server web
- Traffico SMTP/SMTPs, POP3/POP3s, IMAP/IMAPs sul server di posta
- Traffico NTP solo verso alcuni server esterni noti (INRIM, apple)

Schema


INTERNET
GARR
RETE PERIMETRALE
CON SEGMENTAZIONE
Service Oriented Network
RU / FW
FIREWALL
INTERNO
NAT
DMZ
WEB
POSTA
DNS
...
RETE PUBBLICA
DB INTRANET
10.1.x.x
STUDENTI
10.2.x.x
DIPENDENTI
10.3.x.x
GESTIONALI
10.4.x.x

ACL per Cisco (stateful)

```
# Permettiamo prima di tutto le connessioni gia' stabilite
access-list 101 permit tcp any any established


access-list 101 permit udp ip.del.server.DNS.0 0.0.0.255 eq 53


access-list 101 permit tcp ip.del.server.web.0 0.0.0.255 eq 80
access-list 101 permit tcp ip.del.server.web.0 0.0.0.255 eq 443


# Ho VOLUTAMENTE eliminato le porte 25, 110, 143 che non prevedono utilizzo di SSL!!!!
access-list 101 permit tcp ip.del.server.posta.0 0.0.0.255 eq 465
access-list 101 permit tcp ip.del.server.posta.0 0.0.0.255 eq 587
access-list 101 permit tcp ip.del.server.posta.0 0.0.0.255 eq 995
access-list 101 permit tcp ip.del.server.posta.0 0.0.0.255 eq 993

access-list 101 deny ip any any

interface fastethernet 0/1 (interfaccia verso          Internet)
ip access-group 101 in
# Access list per NTP
access-list 50 permit 193.204.114.233
access-list 50 permit 193.204.114.232
access-list 50 permit 193.206.158.0 0.0.0.255
ntp access-group serve 50
ntp access-group query-only 50
```

ACL Juniper (web, mail)

```
firewall {
    filter incoming_traffic {
        term establised_connections {
            from {
                tcp-established;
            }
            then accept;
        term WWW {
            from {
                destination-address {
                    ip.de.server.web/32;
                }
                protocol tcp;
                destination-port [ 80 443 ];
            }
            then accept;
        }
        term MAIL {
            from {
                 destination-address {
                    ip.del.server.mail/32;
                }
                protocol tcp;
                destination-port [465 587 995 993];   # Ho volutamente tolto la 25 110 143
            }
            then accept;
        }
```

ACL per Juniper (NTP)

```
term allow-ntp {
    from {
        source-address {
            193.204.114.233;
            193.204.114.232;
            193.206.158.0/24;
        }
        protocol udp;
        port ntp;
    }
    then accept;
}

term block-ntp {
    from {
        protocol udp;
        port ntp;
    }
    then {
        discard;
    }
}
```

ACL Juniper (DNS)

```
term DNS {
        from {
            source-address {
                ip.del.forwarder.esterno/32;
                ip.del.forwarder.secondario/32;
            }
            protocol udp;
            source-port 53;
        }
        then {
            count DNS;
            accept;
        }
    }
    term other {
        then discard;      # rigetta tutto il resto del traffico
    }
  }
}
}
```

Stateless firewall

- Se il router di bordo non offre funzionalita' di stateful firewalling la configurazione «in sicurezza» potrebbe diventare un inferno
- Non potendo dire: permetti in ingresso tutto quello che e' «established» e' necessario permettere tutto e andare a togliere tutto quello che e' superfluo o addirittura nocivo:
- small-services (echo, chargen, finger, tftp, etc)
- ftp, telnet, rdp, microsoft-share, X11…
- Servono anche due access-list diverse, una in entrata e una in uscita

MIGLIAIA DI REGOLE DA SCRIVERE PUNTUALMENTE!

Stateless Hell

E dopo queste vanno inserite quelle in uscita!!

```
Access-list 111 permit tcp any any estabilished
Access-list 111 deny tcp any any range 1 19
Access-list 111 permit tcp any host server1_di_posta eq smtp
Access-list 111 permit tcp any host server2_di_posta eq smtp
Access-list 111 deny tcp any any eq smtp
Access-list 111 deny tcp any any range 26 52
Access-list 111 deny tcp any any range 54 79 (occhio a sql*net)
access-list 111 deny tcp any any range 135 139
access-list 111 deny tcp any any eq 445
Access-list 111 deny tcp any any range 513 514
access-list 111 deny tcp any any eq 593
Access-list 111 deny tcp any any eq 2049  (NFS)
Access-list 111 deny tcp any any range 6000 6063     (X11)
Access-list 111 deny tcp any any range 6660 6680    (IRC)

Access-list 111 deny udp any any range 1 19
Access-list 111 deny udp any any range 26 52
Access-list 111 deny udp any any range 54 79
access-list 111 deny udp any any range 135 139
access-list 111 deny udp any any eq 445
Access-list 111 deny udp any any range 513 514
access-list 111 deny udp any any eq 593
Access-list 111 deny udp any any eq 2049  (NFS)
Access-list 111 deny udp any any range 6660 6680     ""

Access-list 111 deny ip <ser_ip> 0.0.0.0 <ser_ip> 0.0.0.0
access-list 111 deny ip 127.0.0.0   0.255.255.255 any
access-list 111 deny ip 10.0.0.0    0.255.255.255 any
access-list 111 deny ip 172.16.0.0  0.15.255.255 any
access-list 111 deny ip 192.168.0.0 0.0.255.255 any
access-list 111 deny ip 150.145.1.0 0.0.0.255 any
```

LA RETE INTERNA

Rete interna

- Il router di bordo non ha coscienza ne' della sua esistenza ne' di dove si trovi
- La rete interna non deve essere raggiungibile dall'esterno
- Dalla rete interna si puo' solo uscire
- Le varie sottoreti interne non si devono vedere a meno di esigenze particolari e regole esplicite

Segmentazione

All'interno di una LAN avvengono cose BRUTTE!!

- Minacce di compromissioni
- Spread del malware
- Scansioni LAN, tentativi di connessione
- Raccolta informazioni
- Ransomware
- Cartelle condivise
- Probabilita' elevata di danni
- Difficolta' stabilire patching policy per workstation
- Rischio elevato

Tenere le reti separate ci da' uno strumento in piu' per evitare lo spread incontrollato su reti particolarmente critiche

Segmento Intranet

- Gestionali (presenze, contabilita', stipendi, etc)
- Database
- Eventuale DNS interno
- Server di stampa e stampanti
- Eventuale server di posta interno
- Eventuale server di autenticazione (Es. LDAP, RADIUS etc etc)

Segmento monitoraggio

- E' un segmento a parte perche' la politica per questa rete potrebbe essere piu' aperta rispetto ai server sulla intranet
- A seconda del software delle sonde che usiamo per monitorare potrebbe essere necessario aprire questo segmento di rete anche in entrata
- E' meglio tenerla scollegata dai server sulla intranet
- Questo pezzo di rete raccoglie tutti i dati delle sonde di monitoraggio (log si sistema, sonde NetFlow, log di IDS etc etc)
- In questo segmento sono installati inoltre i software di gestione e visualizzazione ed elaborazione/analisi dei log

Segmento PC Dipendenti

- Leggono posta
- Web
- Possono fare tutto in uscita
- Alcuni di essi possono accedere ad alcuni servizi della intranet
- Costruire una tabella di «chi fa cosa» per configurare le relative regole sul firewall

Segmento PC Studenti

Include anche aule pubbliche e biblioteche

- Devono solo andare fuori e utilizzare i servizi «al pubblico» che stanno in DMZ
- Non devono accedere alla rete intranet
- Considerati come ospiti o external user (Zero Trusted Network)

Segmento PC Laboratori

- Non hanno esigenze diverse dai PC studenti
- Ma e' meglio non mescolarsi con i PC studenti
- Magari ci sono dati particolari, o DB o strumenti di lavoro

Firewall Interno

Switch L3 o macchina linux

Una interfaccia per ogni rete interna + 1 ext

Funzioni di routing

NAT

DHCP

L'idea «piu' sicura» sarebbe attestare ogni rete separata su switch separati che entrano nell'interfaccia di rete appropriata del fw

Regole di routing

Le macchine della rete interna hanno indirizzi privati, segmentati il piu' possibile per utilizzo

Tutti possono andare verso l'esterno

I PC dipendenti possono accedere ai gestionali

- Magari decidere puntualmente dipendente per dipendente

Alcuni PC possono accedere al monitoraggio

Le stampanti di rete?

PC di studenti, aule PC, PC biblioteca

Eventuali PC/server per laboratori di ricerca, o sviluppo

Videosorveglianza

Hardening firewall

Regole per bloccare il traffico su se stesso

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

```
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state NEW,RELATED,ESTABLISHED -j
ACCEPT
```

```
iptables -A INPUT -m state --state NEW -i ! eth1 -j ACCEPT
```

Puo' solo uscire

In ingresso sono permesse connessioni gia' stabilite

Regola di NAT

(S)nattiamo tutto il traffico in uscita dalle sottoreti

iptables -t nat -A POSTROUTING -o eth0 -s 10.0.0.0/8 -j MASQUERADE

In questo caso eth0 e' l'interfaccia verso RU

Regole di routing

- Ruotiamo senza restrizioni in entrata solo quello che e' gia' ESTABLISHED

iptables -A FORWARD -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

- Abilito il PC di Tizio (10.2.0.20, eth2) ad usare il gestionale GESTY (10.1.0.50, port 443, eth1)

iptables -A FORWARD -p tcp -i eth2 -s 10.2.0.20 -o eth1 -d 10.1.0.50 --dport 443 -j ACCEPT

DHCP

Assegnazione statica di indirizzi IP

Alla DMZ vengono assegnati IP pubblici ovviamente statici

- Inseriti nel DNS primario

Alla rete interna verranno assegnati

- IP statici privati per la rete intranet dei server
- IP statici via DHCP per tutti gli altri
    - Nella sottorete opportuna a seconda dell'utilizzo

Vantaggi DHCP

- Unico file di configurazione con lo stato dell'arte di tutti gli IP assegnati
- Accesso non anonimo alla rete
- Assegnazione centralizzata di DNS e GW

E una cosa che non fa mai nessuno ma e' fondamentale:

- Regola di blocco: chi non e' registrato non va

Hardening DHCP

Dire che vogliamo essere l'unico DHCP della sottorete

authoritative;

deny unknown-clients;

La prossima direttiva VIOLA l'RFC del protocollo ma e' utile per evitare doppioni di IP sullo stesso MAC address

deny duplicates;

Tempo di rinnovo IP

default-lease-time 600;

max-lease-time 7200;

Configurazione assegnazione IP

```
# Definizione di una sottorete (PC dipendenti) e dei suoi specifici parametri

group {
        option routers 10.2.0.1
        option subnet-mask 255.255.0.0
        option domain-name-servers 192.84.145.20
        option domain-name dip.uniXX.it
        host tizio {
                hardware ethernet 00:AA:FF:44:33:33
                fixed-address 10.2.0.10
        }
        host beppo {
                hardware ethernet DD:DD:DD:DD:DD:DD
                fixed-address 10.2.0.11
        }
}
```

Regola salvavita

Inserire nel firewall una regola che permetta soltanto agli IP registrati di andare in internet (che si trova su eth0, non forwardiamo verso la rete interna!!!)

iptables -A forward -i eth2 -s 10.2.0.10 -o eth0 -j ACCEPT

iptables -A forward -i eth2 -s 10.2.0.11 -o eth0 -j ACCEPT

NB: Va fatto per ogni host registrato nelle sottoreti!

Non e' oneroso se quando si edita il dhcpd.conf si aggiunge anche la regola iptables

Si puo' fare anche automaticamente con 1-2 righe di bash

Eventuali problemi

- Configurazione semplice
- Sufficientemente sicura e robusta
- Evita che qualcuno arrivi, prenda un indirizzo di rete e inizi a navigare a nostra insaputa

…. A parte LUI!!!

Il pericolo!!!

1. Mi attacco all'HUB
2. Il DHCP non mi da' niente
3. Posso sniffare tutto il traffico che passa a livello2 (ARP, DHCP Request.. Etc etc)
4. Scopro la rete e la netmask
5. Mi assegno da solo un IP sulla rete
6. Vedo che non navigo fuori (regola salvavita!)
7. Ma posso sniffare tutto dentro a livello3!!!

Minacce

1. Posso sniffare i MAC address registrati e rubarne uno
2. Posso sniffare tutto il traffico di quella sottorete
3. Posso scannare tutta la sottorete in cerca di vulnerabilita' e prendermi direttamente un PC
4. Se la rete non e' segmentata anche a livello2 o fisico, posso sniffare i pacchetti ARP anche delle altre sottoreti e collegarmi a quelle

LA INTRANET!!!!! I SERVER!!!!

Attacchi livello 2-2.5

Non e' materia da corso basico. Due soluzioni possibili:

1. Controllare il traffico a livello2 tramite switch managed con funzionalita' VLAN e/o in grado di filtrare pacchetti ARP (arptables).
   a. Bello, concettualmente semplice, pulito.
   b. Difficile gestione e costoso

2. Installare sul firewall interno un programma di monitoraggio ARP (arpwatch) che avvisa quando cambia il MAC address associato abitualmente ad un IP.

   Poi ci alziamo e andiamo a vedere chi e'!

DNS

DNS

Il DNS e’ un servizio fondamentale per la raggiungibilita’ di una struttura

Protocollo UDP porta 53

Esposto al pubblico

E’ un servizio molto delicato

Largamente utilizzato per diversi tipi di attacchi

Tipi di attacchi (1)

Rerouting di tutto il traffico di un PC verso reti o host malevoli tramite injection di DNS server sui PC client

Soluzione

Obbligare i PC ad usare il DNS istituzionale

- Tramite DHCP DNS push
  - option domain-name-servers ip.del.server.DNS
- Blocco su RU in uscita di tutto il traffico DNS escluso il server istituzionale
  - access-list 101 permit udp ip.del.server.DNS.0 0.0.0.255 eq 53

Tipi di attacchi (2)

DoS DDoS DrDoS: attacchi che usano il DNS come vettore per perpetrare Denial of Service

- *Non e' una compromissione del DNS*

Configurazione troppo aperta: il DNS risponde a qualsiasi query da qualunque posto venga con un pacchetto verso la vittima che puo' avere un fattore di amplificazione di migliaia di volte

Per pochi byte di richiesta vengono spediti Kbyte alla vittima

Soluzione

Restringere la possibilita' di fare query al DNS solo alla propria rete

Impedire la recursione verso la rete esterna sia sul router (UDP/53 e TCP source port 53) che in configurazione

Tipi di attacchi (3)

Esposizione di dati sensibili

Caso in cui il DNS e' malconfigurato e invia informazioni sulla propria zona o parte di essa a chiunque

Addirittura effettua un vero e proprio zone-transfer verso macchine o reti non abilitate

Soluzione

Chiudere la configurazione troppo aperta

Architettura servizio DNS

Dove lo mettiamo?

Come forniamo in maniera piu' sicura il servizio DNS?

2 possibili soluzioni:

1. Unico server in DMZ che serva sia la parte pubblica che quella privata
2. Un server in DMZ autoritativo per la zona pubblica, interrogabile dall'esterno e un server nella intranet, autoritativo per la zona privata, interrogabile dall'interno

Possibilita' n. 1 - DNS interno ed esterno

Il DNS esterno e' autoritativo per la rete pubblica ed e' interrogabile solo dall'esterno

Il DNS interno e' autoritativo per la rete interna, e' interrogabile da tutti i client in rete privata e funziona da cache/forwarder per tutte le richieste interne che non comprendono la rete interna

Vantaggi: Tengo separate le due zone

Non espone la lista delle macchine interne ad eventuali attaccanti esterni

Svantaggi: Devo aprire una breccia nella intranet in ingresso!

Dobbiamo inserire sul firewall interno una regola che permetta l'inoltro di pacchetti DNS da tutti la rete privata, di qualsiasi segmento, verso il DNS interno (e una per consentire il routing interno verso la rete intranet, eth1, per connessioni ESTABLISHED)

Dettagli - DNS interno ed esterno

Apro la breccia sulla intranet:

```
iptables -A FORWARD -i eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -proto udp -s 10.0.0.0/8 -d ip.del.DNS.INTERNO --dport 53 -j ACCEPT
```

Possibilita' n. 2 - Unico DNS

Vantaggi

- Soluzione piu' semplice e robusta
- Unico punto delicato da gestire
- Nessuna regola ulteriore per la rete interna

Svantaggi

La configurazione della zona interna e' esposta al pubblico, va tenuto d'occhio con gli aggiornamenti e vulnerabilita'

(ma tutto sommato anche se riescono a scoprire gli IP della rete interna non e' che poi se ne possono fare gran che)

Esempio: Configurazione ISC bind

Definizione ACL per accesso al DNS

```
acl "xfer" { none; };
acl "trusted" {
        192.84.145.0/24
        localhost;
        };
acl " client-interni" { 10.0.0.0/8;};
acl "intranet" {10.1.0.0/16;};
options {
        allow-transfer { xfer;};
        allow-query { trusted, client-interni; };
        allow-query-cache { trusted, client-interni; };
};
```

ISC bind

Vista rete pubblica accessibile da tutta internet
(ho omesso la zona «root server» e «localhost»)

```
view "external-in" in {
        match-clients { any; };
        recursion no;
        additional-from-auth no;
        additional-from-cache no;
        zone "uniXX.it" in {
                type master;
                file "master/db.example";
                allow-query {
                any;
                }; };
        zone "145.84.192.in-addr.arpa" in {
                type master;
                file "master/db.145.84.192";
                allow-query {
                any;
                }; };
};
```

ISC bind

Vista rete interna - accessibile solo da interni

(ho omesso la zona «root server» e «localhost»)

```
view "internal-in" in {
match-clients { trusted, intranet; };
recursion yes;
additional-from-auth yes;
additional-from-cache yes;
zone "intranet.uniXX.it" in {
        type master;
        file "master/db.internal";
};
zone "1.10.10.in-addr.arpa" in {
        type master;
        file "master/db.10.10.1";
        };
};
```

AUTENTICAZIONE

Servizi di AAA

Autenticazione, autorizzazione, accounting

Ogni applicativo dell'istituzione prevede piu' o meno un sistema di autenticazione per accedere

Nella preistoria ognuno di questi aveva un proprio database interno locale da interrogare, sia per l'autenticazione che per l'autorizzazione

In tempi piu' moderni le architetture si sono evolute verso un sistema di SingleSignOn, che permette la gestione centralizzata delle informazioni relative agli utenti e che consenta la gestione dei dati sia in maniera affidabile, con i dati sempre aggiornati, sia in maniera piu' controllata, per garantire una maggior sicurezza dei dati

SingleSignOn: sistema di autenticazione, autorizzazione, accounting in cui si mette una volta sola la coppia utente/password e serve per accedere a piu' servizi autenticati senza doverla inserire piu' volte

La cosa figa e' che in questo caso e' che sulla rete non passano piu' password, ne' informazioni di autenticazione, ne' attributi ne' dati, solo un ID anonimo di sessione «gia' autenticata»

Tecnologie di AAA

Autenticazione

- Form/Basic Autentication
- Kerberos
- Certificati digitali
- SmartCard o TokenUSB
- LDAP
- RADIUS
- CAS
- OpenID e/o SAML

Autorizzazione

- LDAP
- SAML
- Oauth
- Federazioni

I servizi autenticati

Posta elettronica

wi-fi e/o eduroam

Gestionali interni

Web esterni e interni

- Moodle
- Applicativi web di qualsiasi tipo
- Forum

NB: Nel caso di utenti esterni che si registrano per forum o altro ma che non abbiano attinenza con la struttura si consiglia di utilizzare fattori di autenticazione esterni (tipo Google o Facebook) in modo che le problematiche di sicurezza e privacy vengano gestite da loro. Non vedo l'utilita' di sprecare risorse per registrare sui propri sistemi username e dati di persone che non fanno parte ad alcun titolo della struttura

Suddividere per utenza

- Stabilire chi deve accedere a cosa
- Mettere i servizi il piu' possibile «vicino» agli utenti (esempio: se acceduto solo da studenti o da un laboratorio metterlo direttamente li')
- Mettere in DMZ quelli accedibili dall'esterno
- Mettere in intranet quelli accedibili solo dall'interno
- Suddividere i servizi offerti via web secondo questo criterio

Attacchi ad LDAP in DMZ

Server web che saranno costantemente bombardati in cerca di falle (php, malconfigurazioni, SQL Injection… Basta leggersi il rapporto OWASP sulle maggiori wulnerabilita' web)

Intercettazione delle password in chiaro

- USARE SSL SEMPRE DOVUNQUE E COMUNQUE

Attacchi a forza bruta

- Stabilire delle policy per la gestione delle password (vita di una password, lunghezza)

Dove piazzare l'autenticazione

Come per il DNS le soluzioni sono due

- 1 LDAP unico accedibile da tutti
- 2 LDAP, uno in DMZ per i server in DMZ e uno in intranet per i server in intranet

In questo caso e' consigliabile la seconda soluzione

Architettura LDAP

Un LDAP master in intranet

- Raggiungibile e leggibile solo dalle applicazioni in intranet
- Scrivibile solo da utenti e/o applicazioni puntuali

Un LDAP slave in DMZ

- Raggiungibile e leggibile solo dalle applicazioni in DMZ
- **Non scrivibile!!! (replica in sola lettura)**

Il protocollo di comunicazione fra i due server e' LDAPS (SSL) - TCP/636

La direzione di comunicazione e' da intranet verso DMZ

NON DOBBIAMO APRIRE IL FIREWALL!!

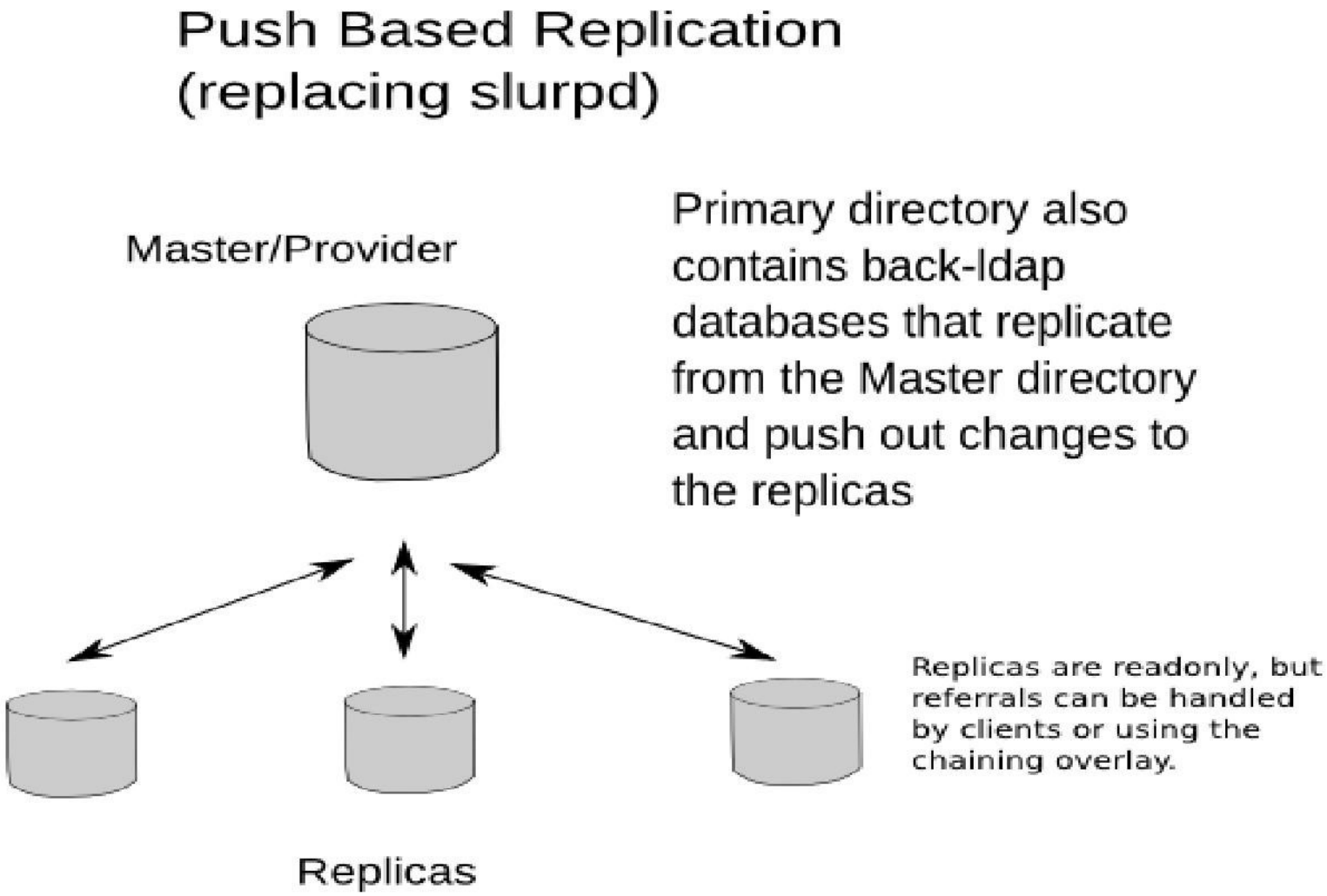
Configurazione LDAP Master/Slave

Con la versione 2.4 di LDAP e' cambiata tutta l'architettura delle repliche, permettendo molti piu' tipi di configurazioni master/slave, sia per failover, che HA, sia multi-master

Si chiamano Provider/Consumer

- Non esiste piu' slurpd
- Al suo posto c'e' syncrepl
  - Sviluppato per garantire la sincronia in tempo reale, ma non per la sicurezza
  - Non permette di default la possibilita' di comunicare a senso unico verso il consumer (e' bilaretale e andrebbe aperto fw)
  - Si riesce a raggiungere un'architettura puramente push-based (che parta solamente in uscita dal Provider) tramite LDAP Backend e uno slapd ldap proxy

Configurazione push-based (fonte LDAP.org)



BACKUP

Backup

Le misure minime di sicurezza ci chiedono:

- Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.

- Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.

Pianificazione Backup

Decidere cosa backuppare

- Server Linux e Windows
  - Sistema operativo e dati/applicazioni/db
  - Solo dati/applicazioni/DB
- Workstation Linux e Windows solo dati e solo dipendenti
- Apparati di rete
  - Flash (sistema operativo) e configurazione
  - Solo configurazione
- Altro?

Decidere dove backuppare

- Server Remoto con attached storage
- NAS

Decidere come backuppare

- Centralizzare il sistema di backup dove il BackupServer comanda tutto
- Sceglie il client quando
- Backup completi o incrementali

Suggerimenti: Cosa backuppare

Server linux - sia SO che applicazioni che dati

- rsync over ssh su BackupServer remoto
- Incrementale 1 volta al giorno
- Completo 1 volta a settimana

PC workstation di utenti - linux e windows

- Solo dati

Apparati di rete

- Salvare la configurazione su BackupServer remoto soltanto quando viene cambiata
- Se la rete e' semplice e gli switch non hanno particolari configurazioni e' sufficiente salvare solo la configurazione di RU

Per una piccola rete: Come Backuppare

BackupServer linux con attached storage

- Script rsync gestiti via cron per i server linux
  (rsnapshop, Duplicity.. Sono cmq interfacce a rsync)
- Samba server per le workstation dipendenti
- (WindowsBackup per server windows)
- scp per configurazione di RU ove possibile
  - TFTP ove non possibile

Se RU e' Cisco o Juniper

Se RU e' aggiornato alle ultime versioni di SO

Hanno implementato un server ssh su cui copiare sia la flash che la configurazione da remoto

Sicurezza

Dove mettiamo il SambaServer

- Possono accedere solo i PC dei dipendenti

  Quindi solo le reti 10.2.0.0 (o eventualmente altre)
- Lo mettiamo in intranet
- Abilitare il forward fra le interfacce coinvolte di fw

iptables -A FORWARD -s ip.singolo.PC.dipendenti -d ip.del.Samba.server -p tcp -dport 445 -j ACCEPT

(«dovrebbe» bastare)

Samba Ports (fonte Microsoft)

Protocols and Ports	Usage	Type of Traffic
TCP and UDP 389	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP
TCP and UDP 88	User and Computer Authentication, Forest Level Trusts	Kerberos
TCP and UDP 53	User and Computer Authentication, Name Resolution, Trusts	DNS
TCP and UDP 445	Replication, User and Computer Authentication, Group Policy, Trusts	SMB,CIFS,SMB2
TCP 135	Replication	RPC
TCP 5722	File Replication	RPC, DFSR (SYSVOL)
UDP 123	Windows Time, Trusts	Windows Time
TCP and UDP 464	Replication, User and Computer Authentication, Trusts	Kerberos change/set password
UDP Dynamic	Group Policy	DCOM, RPC, EPM
UDP 138	DFS, Group Policy	DFSN, NetLogon, NetBIOS Datagram Service
TCP 9389	AD DS Web Services	SOAP
UDP 67 and UDP 2535	DHCP	DHCP
UDP 137	User and Computer Authentication,	NetLogon, NetBIOS Name Resolution
TCP 139	User and Computer Authentication, Replication	DFSN, NetBIOS Session Service, NetLogon

Sicurezza: Dove Backuppare

Dove mettiamo il BackupServer

Lo mettiamo in intranet ma dobbiamo scegliere la soluzione in base a quallo che dobbiamo salvare

- Se il software supporta rsync/scp ce lo prendiamo dalla intranet senza aprire niente con facilita'
- Se il software non supporta rsync dobbiamo prevedere una architettura «di appoggio»
  1. Architettura proxy-backup (Linux) in DMZ - come per i log: facciamo un backup in rete locale e lo prendiamo con rsync *(v. oltre - capitolo LOG)*
  2. Aprire una porta verso la intranet dalla DMZ (sconsigliato)

LOG

LOG server

Evitare di tenere i log di sistema sulle macchine che li producono: se viene compromessa la macchina vengono cancellate le tracce nei log!

Spedire LOG ad un server remoto e' utile anche per il sistema di monitoraggio

Punto delicato della rete: dati appetibili dal punto di vista dell'hacker

E sensibili

Pianificazione

Stabilire cosa vogliamo loggare

- Solo i syslog server
- Log di applicazioni
- Apparati di rete
- Workstation?

Stabilire come lo vogliamo ruotare

Stabilire quanto li vogliamo tenere

- In ottemperanza anche alle leggi vigenti

Stabilire le politiche di accesso ai LOG

- Per troubleshooting
- Per monitoraggio
- Per forensic

A seconda della quantita' e del tipo di dati possiamo scegliere la soluzione migliore

Ente piccolo: cosa

Syslog dei server

- Server in DMZ
- Server in intranet

Applicativi sui server

- Configurabili per loggare via syslog
- Prelevabili tramite cron e rsync su ssh

syslog di apparati di rete (da valutare)

- Servono soprattutto per il monitoraggio di rete e anomalie di traffico, sia malevole che no

Soluzioni possibili

Le soluzioni dipendono anche dalla struttura fisica della rete. In linea generale ci sono due filosofie:

1. **Tenere il LOG server su una rete separata e spargli tutti i log di tutte le macchine singolarmente**
   - Facile da configurare
   - Molto poco scalabile
   - Il traffico degli apparati di rete (UDP/514) passa in chiaro!!!
   - Occorre aprire il firewall interno in entrata (TCP e UDP 514)
2. **Tenere il LOG server su una rete separata inaccessibile**
   - Leggermente piu' complicato da gestire in partenza
   - Scalabile a piacere, semplice delegare la gestione di segmenti
   - Il traffico in chiaro viene incapsulato in un reverse tunnel ssh
   - Nessuna porta da aprire sul firewall interno in entrata

Come scegliere

L'ago della bilancia e' se vogliamo loggare gli apparati di rete o no

- Al momento gli apparati di rete ancora non supportano il protocollo rsyslog ma funzionano ancora con il vecchio syslog remoto
  - Trasmettono solo UDP/514 verso il log server
  - Non supportano TCP, ne' TLS

Ma in fase di monitoraggio di rete i LOG servono!

Soluzione proposta

1 collettore rsyslog (proxy-log) per ogni segmento di rete

- Situato nella sottorete che genera i log

1 log server

- Situato in un segmento apposito «Monitoraggio»
- Raccoglie gli rsyslog dei proxy-log

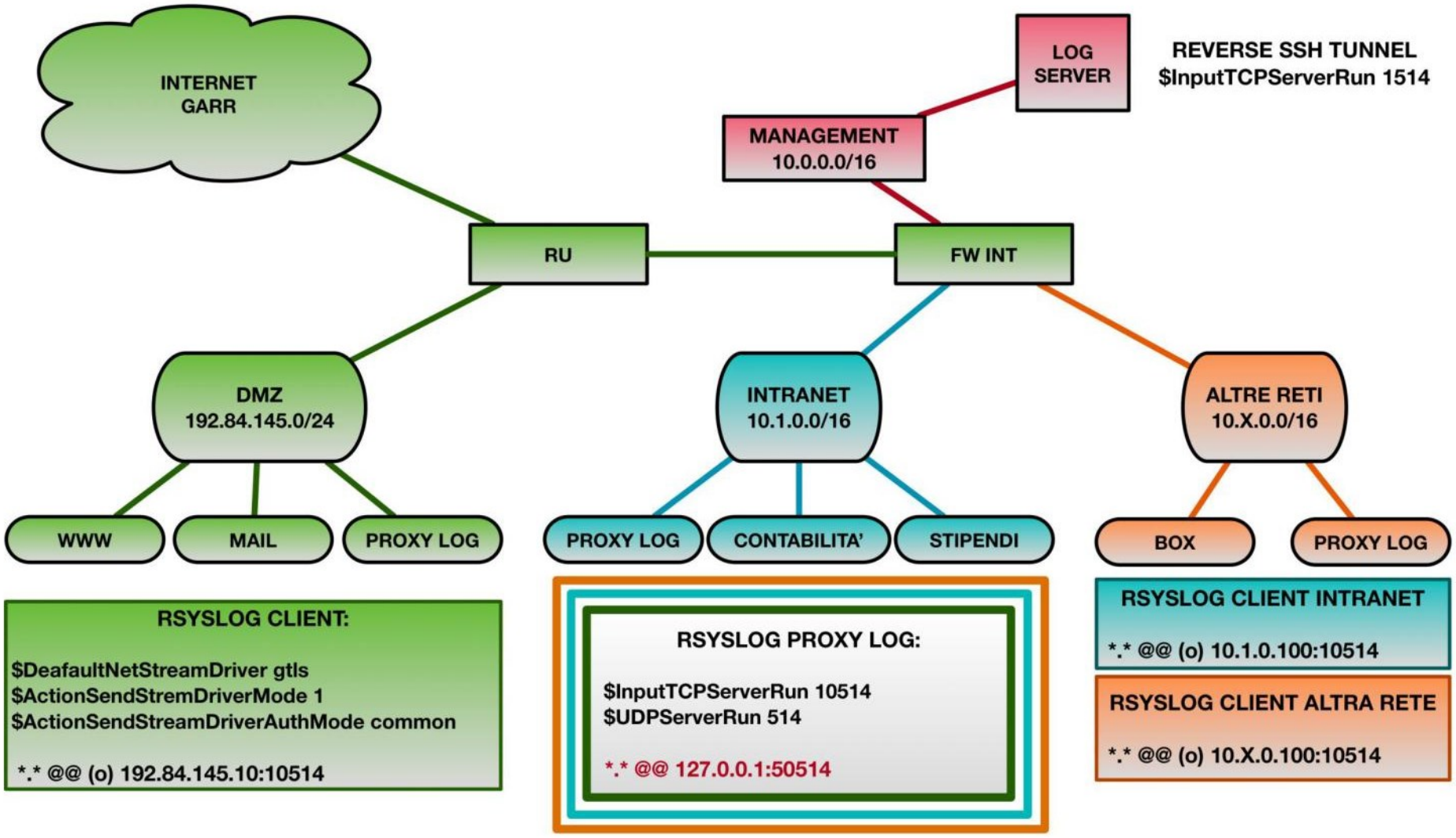
In questo modo i vari server i propri log al loro proxy-log su rete locale

- Via TCP incapsulato TLS per i server
- Via UDP/514 per gli apparati di rete

I vari proxy-log inviano tutto quanto al LOG server attraverso un reverse SSH tunnel

- Tutto il traffico verso il LOG server e' criptato, anche i log degli apparati di rete
- La comunicazione LOGServer <-> proxy-log viene effettuata e gestita dal LOG server, che si va a prendere i log sui proxy-log: non e' quindi necessario aprire il firewall interno in entrata

Sistema di LOG remoto



Cenni di configurazione Client

Client apparati di rete:

Non si accorgono di niente va solo specificato come log server il rispettivo proxy-log

- Esempio per Cisco:

  logging trap debugging <NOME LOG FILE>

  logging facility logging <IP PROXY-LOG>

Configurazione Client «moderni»

Per i client che supportano rsyslog e' preferibile spedire i log al proxy-log attraverso un canale criptato via TCP

Creare un certificato per proxy-log e copiarlo nel client

Configurare la modalita' di trasporto: TLS over TCP utilizzando il certificato del proxy-log

$DefaultNetstreamDriver **gtls**

$ActionSendStreamDriverMode 1
$ActionSendStreamDriverAuthMode anon

***.* @@(o)IP.del.proxy.log:10514**

Configurazione Proxy-log - raccolta log dei client

Copiare il proprio certificato e la CA e metterli nel file di configurazione rsyslog.conf

Configurare la parte TLS per ricevere i log delle macchine sulla porta TCP/10514

$DefaultNetstreamDriver gtls

$ModLoad imtcp $InputTCPServerStreamDriverMode 1

$InputTCPServerStreamDriverAuthMode anon

$InputTCPServerRun 10514

Per finire accogliamo anche il traffico degli apparati di rete «alla vecchia maniera»

$InputUDPServerBindRuleset remote

$UDPServerRun 514

Configurazione Proxy-log e LOGServer

Questa procedura va ripetuta per ogni proxy-log

Creiamo su proxy-log e LOGServer un utente rslr e installiamo le relative chiavi ssh in authorized_key per permettere l'accesso ssh bidirezionale solo tramite chiave

Configuriamo proxy-log per spedire i log a se stesso sulla porta del reverse SSH tunnel

***.* @@127.0.0.1:50514**

Creiamo il reverse SSH tunnel su LOGServer (da far partire al boot)

*sudo -u rsyslog-remote ssh -nN -R **50514**:logserver.uniXX.it:1514 proxy-log.uniXX.it*

Configuriamo LOGServer per ricevere anche questi log

$InputTCPServerRun 1514

Regola FW interno

Con questa configurazione la DMZ e' a posto e non c'e' da fare altro (nessuna porta aperta!!!)

Inoltre, dato che la policy di default per il FORWARD e' DROP, dobbiamo istruire FW interno ad instradare i pacchetti che arrivano da LOGServer sulle interfacce appropriate delle sottoreti 10.x. Supponendo che l'ip del LOGServer sia 10.0.0.100 (su eth4) e l'ip del proxy-log sia 10.X.0.100 (ethX)

iptables -A FORWARD -s 10.X.0.100 -d 10.0.0.100 -m state --state RELATED,ESTABLISHED -j ACCEPT

iptables -A FORWARD -p tcp -i eth4 -s 10.0.0.100 --sport 1514 -o ethX -d 10.X.0.100 --dport 10514 -j ACCEPT

E non abbiamo aperto nessuna breccia sulla intranet!

MONITORAGGIO

Monitoraggio

Log di sistemi

Log di rete

DNS log

Sonde IDS (Suricata, Snort)

Eventuale NetFlow

…

Collezionate tutte sul MonitorServer sul segmento «Management»

Analisi ed elaborazione:

Logstash && Elastic Search && kibana

LogStash

Centralize, Transform & Stash Your Data

- Prende in input tutti i log possibili simultaneamente
- Li trasforma al volo e li normalizza in un formato standard uguale per tutti
- Li passa allo «stash» - programma di analisi ed elaborazione dei dati

ElasticSearch

Search and analytics engine capable

- Esegue query di qualsiasi tipo sui dati
- Analisi dei dati
- Aggregazione
- Correlazione

Kibana

Your Window into the Elastic Stack

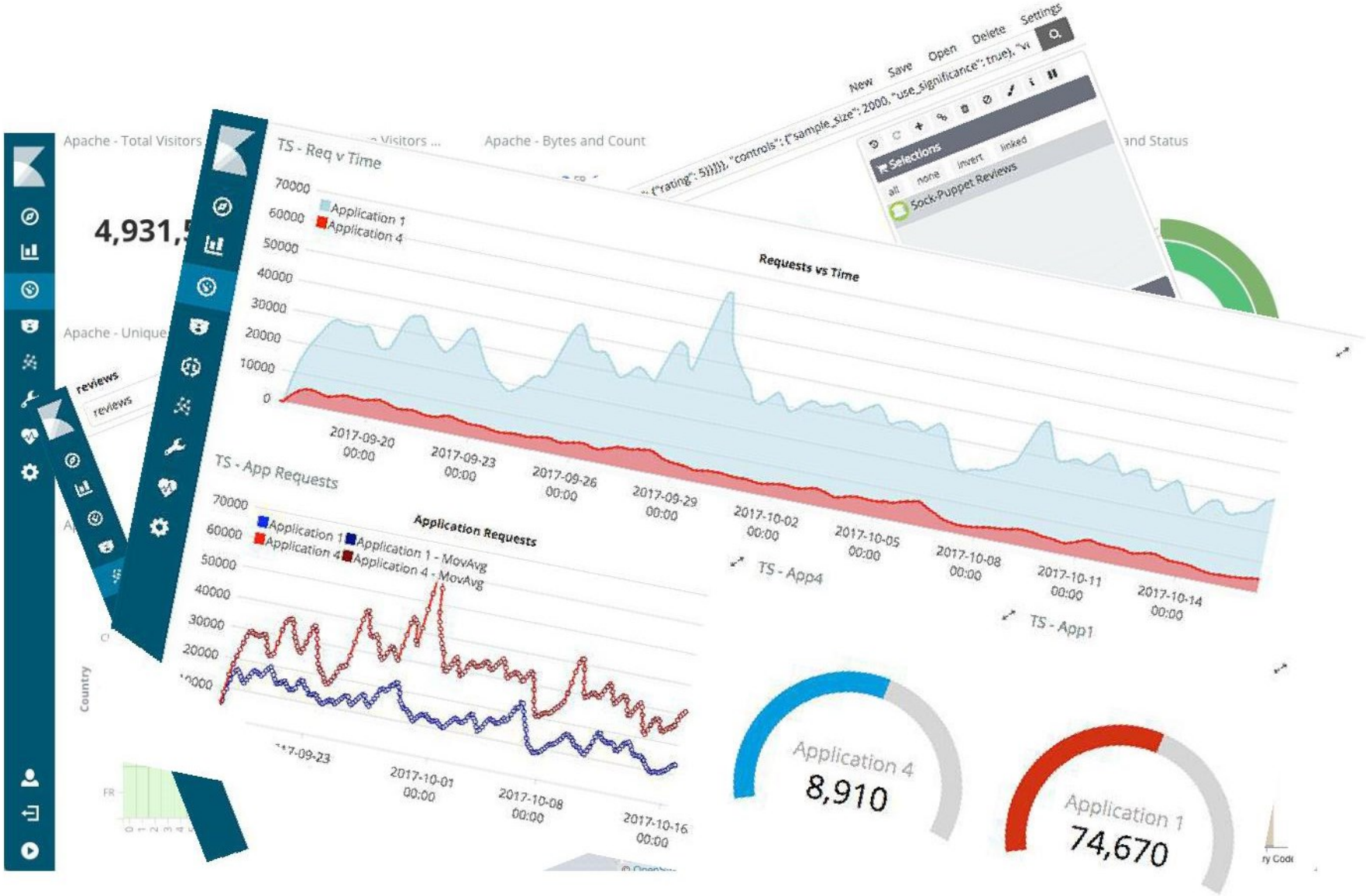
- Visualizzazione dei dati
- Grafici
- Report
- Allarmi

LS & ES & KB

- Performance altissime: non consuma risorse
- Puo’ stare sulla stessa macchina del LOGServer
- Scala orizzontalmente (per scalare basta aggiungere hardware)
- Migliaia di plugin per analizzare sia i log di sistema che i log di rete che NetFlow…
- Tutto grafico!
- Report, allarmi via mail o SMS

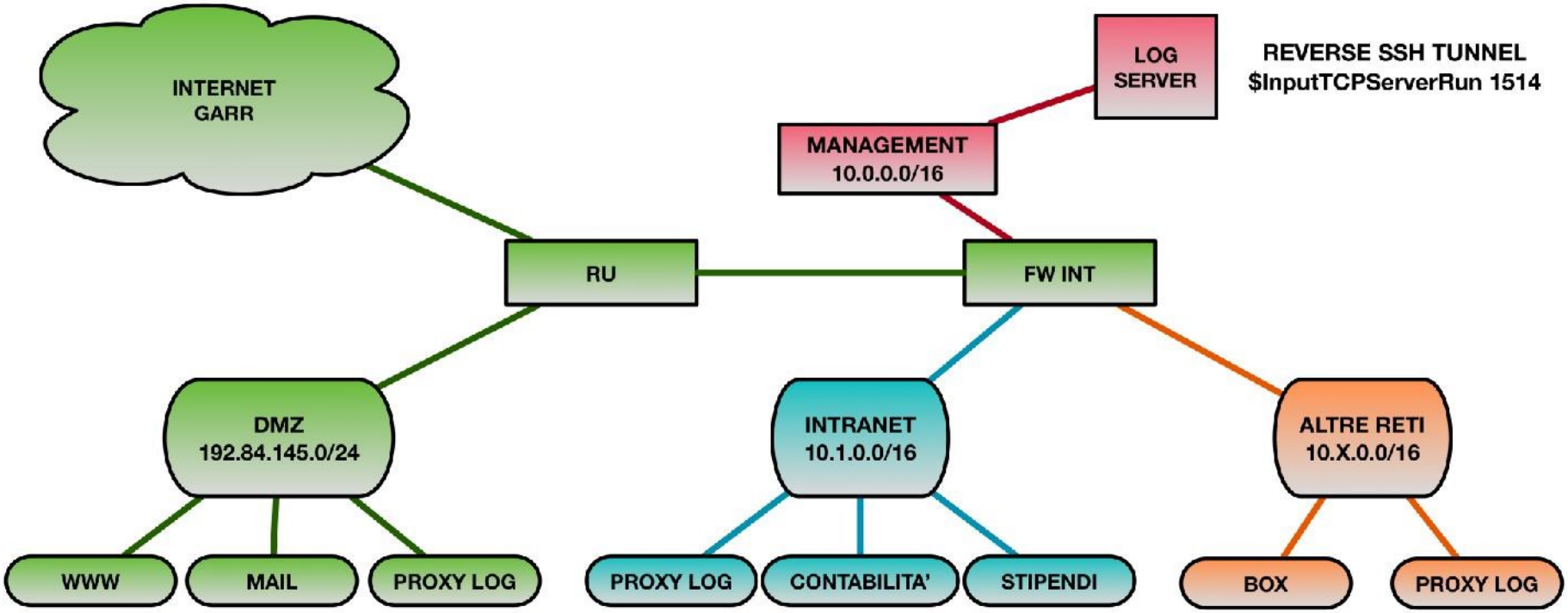

Apache - Total Visitors
4,931,584
Apache - Unique Visitors
29,740
Apache - Unique Visitors ...
City
Unique Visitors
Beijing 562
Redmond 445
Ashburn 400
Chicago 373
Los Angeles 245
Seattle 233
San Jose 232
Singapore 208
Apache - Bytes and Count
US FR DE NL CN
Count
30,000
20,000
10,000
2017-09-23 20:00
2017-09-30 20:00
2017-10-07 20:00
@timestamp per 3 hours
Apache - Country and Status
Apache - Country traffic by hour
US
CN
DE
GB
FR
Country
Hour of Day
Apache - Visitor Map (geocentroid)
Apache - Browser to Country (vega)
4,500,000
4,000,000
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
Chrome
Firefox
Googlebot
IE
Other
CN
DE
FR
GB
NL
US
Agent
Country Code


Apache - Total Visitors
4,931,584
Apache - Unique Visitors ...
City
Unique Visitors
Beijing 562
Redmond 445
Apache - Bytes and Count
US FP
Apache - Unique Visitors
reviews
reviews
New Save Open Delete Settings
Selections
all none invert linked
Sock Puppet Reviews
% Link summary
71816 187
1 (!) 1260
Country
CN
DE
GB
FR
DE
FR
GB
NL
US
Googlebot
IE
Other
2,000,000
1,500,000
1,000,000
500,000
0
Agent
Country Code


Apache - Total Visitors
Apache - Bytes and Count
Apache - Unique
TS - Req v Time
Application 1
Application 4
Requests vs Time
TS - App Requests
Application Requests
Application 1 - MovAvg
Application 4 - MovAvg
TS - App4
TS - App1
Application 4
8,910
Application 1
74,670
New
Save
Open
Delete
Settings
Selections
Sock-Puppet Reviews
reviews
Country


Apache - Total Visitors
4,931,584
Apache - Unique Visitors
29,740
Apache - Unique Visitors ...
City
Unique Visitors
Beijing 562
Redmond 445
Ashburn 400
Chicago 373
Los Angeles 245
Seattle 233
San Jose 232
Singapore 208
Apache - Bytes and Count
US FR DE NL CN
Count
@timestamp per 3 hours
Apache - Country and Status
Apache - Country traffic by hour
Country
Hour of Day
Apache - Visitor Map (geocentroid)
Apache - Browser to Country (vega)
Chrome
Firefox
Googlebot
IE
Other
CN
DE
FR
GB
NL
US
Agent
Country Code
TS - Req v Time
Application 1
Application 4
TS - App1
TS - App4
TS - App Requests
Application Requests
Application 1 - MovAvg
Application 4 - MovAvg
Application 4
8,910
Application 1
74,670

La mia rete


INTERNET
GARR
LOG
SERVER
REVERSE SSH TUNNEL
$InputTCPServerRun 1514
MANAGEMENT
10.0.0.0/16
RU
FW INT
DMZ
192.84.145.0/24
INTRANET
10.1.0.0/16
ALTRE RETI
10.X.0.0/16
WWW
MAIL
PROXY LOG
PROXY LOG
CONTABILITA'
STIPENDI
BOX
PROXY LOG

SCANSIONI

Scansioni vulnerabilita'

Le misure minime di sicurezza chiedono di effettuare delle scansioni di vulnerabilita' periodiche sulle proprie macchine

- Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
- Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
- Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio

WIFI

Wifi & BYOD

Offriamo il servizio wifi per permettere la connessione in rete a ospiti temporanei, eventi o persone che utilizzano i propri dispositivi invece di quelli forniti dalla struttura (BYOD=Bring Your Own Device)

Questi tipi di dispositivi *non appartengono al nostro ente* e non possiamo

- Forzare l'utilizzo o il non utilizzo di certo software, tipo l'antivirus
- Forzare l'utente a adeguarsi alle policy in fatto di software e aggiornamenti
- Intervenire in caso di problemi
- Impedire che portino malware a casa nostra e tentino di infettare tutto quanto

Apriamo le ostilita'

La rete wireless deve essere considerata una rete «ostile», al pari di internet

Gli utenti che si collegano devono essere considerati come utenti esterni alla nostra rete e usufruire soltanto dei servizi «pubblici»

Per questo motivo devono stare su un segmento di rete al di fuori della intranet

Anche al di fuori del nostro fw-int

Autenticazione

Lo scopo e' sempre quello di non fornire accessi anonimi

- A volte gli utenti che si collegano sono studenti o dipendenti, comunque persone che hanno gia' delle credenziali SSO valide sul nostro sistema di autenticazione

- A volte solo solo ospiti temporanei, oppure account provvisori forniti in occasione di eventi o convegni

Soluzioni possibili

Le soluzioni possibili sono tantissme

Ne presento una di facile implementazione e piuttosto robusta

- Si basa sulla distribuzione «zeroshell»
- Autenticazione e cifratura del traffico tramite WPA/WPA2 Enterprise
- Credenziali verificate mediante un server RADIUS con protocollo 802.1x

Zeroshell

Distribuzione LIVE Linux pensata per fornire tutti gli strumenti necessari alla gestione di una rete (firewall, NAT, DNS, wireless etc etc)

- Puo' fare anche da router o bridge trasparente sulla rete
- Captive portal
- Proxy con funzionalita' antivirus
- Server RADIUS
- VPN

..... Migliaia di funzionalita'

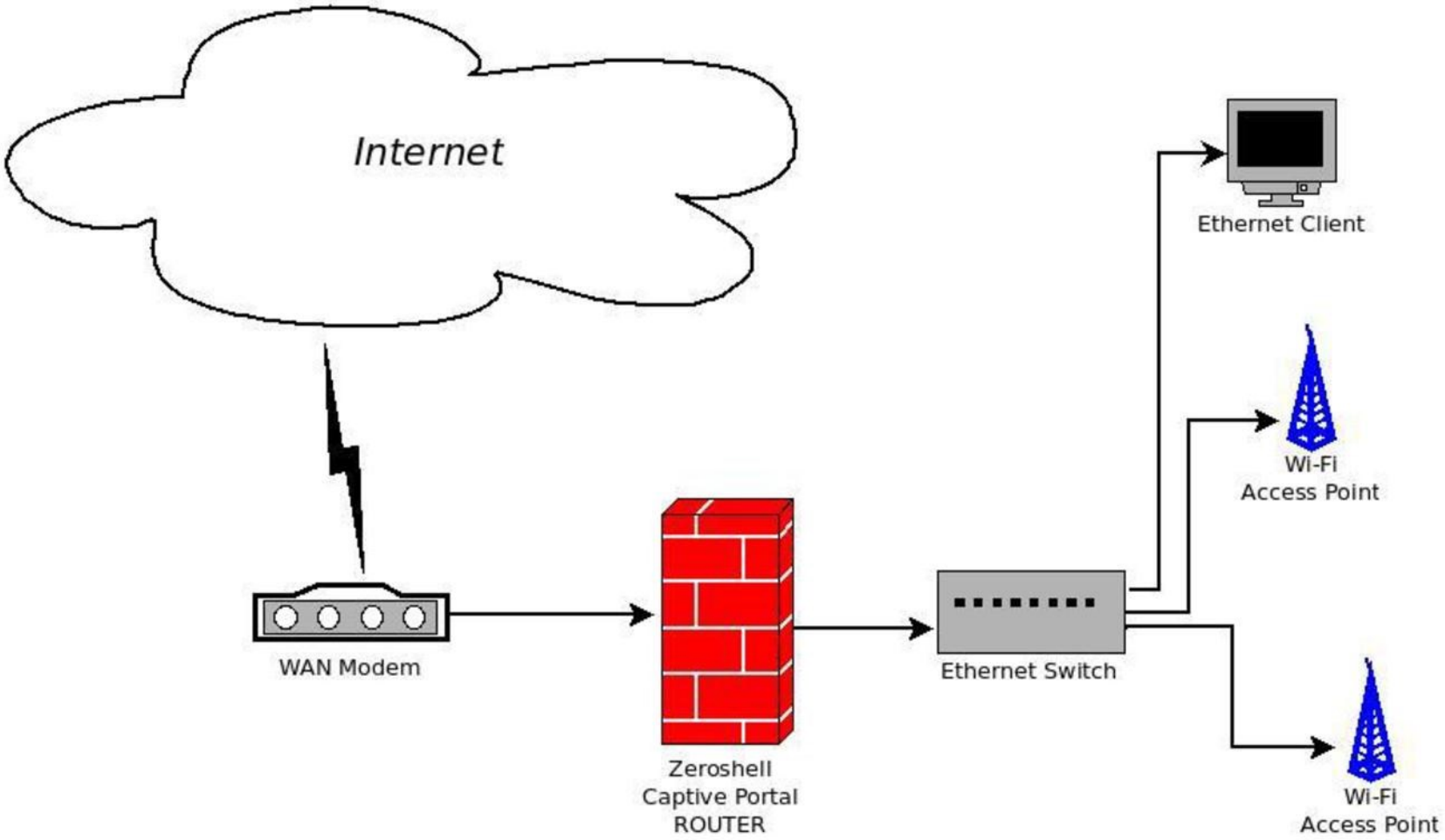
HotSpot Router

Nel nostro caso utilizzeremo zeroshell come HotSpot router per la rete wireless

Fornisce il sistema completo per Autenticazione, Autorizzazione, Accounting

- Strumenti di autenticazione non anonima
- Registrazione degli accessi nei log
- Accounting del traffico

Architettura (fonte ZeroShell)



Autenticazione

- Mediante password e/o certificato digitale X.509
- Autenticazione e cifratura del traffico tramite WPA/WPA2 Enterprise
- WPA/WPA2 Enterprise prevede che gli Access Point Wi-Fi associno un client solo se l'utente ha delle credenziali valide verificate mediante un server RADIUS con protocollo 802.1x. Oltre all'autenticazione, è garantita anche la cifratura del traffico tra client ed Access Point.

Il server RADIUS

L'autenticazione RADIUS avviene tramite il protocollo

- TLS EAP-TTLS
- TLS PEAP + MSCHAPv2

Senza entrare nei dettagli a interessa sapere che possiamo autenticare i nostri utenti

- Attraverso certificati digitali X.509
- Attraverso utente e password inseriti in RADIUS

X.509

Zeroshell ha gli strumenti per crearsi una CA e certificati digitali, ma non sono riconosciuti da alcuni supplicant microsoft

E' necessario installare il certificato della CA e renderlo attendibile ---> sui PC degli utenti e' una operazione difficile che puo' creare problemi

Si possono utilizzare i certificati digitali forniti gratuitamente da Google tramite il servizio TCS

- Hanno la CA universalmente riconosciuta (DigiCERT)
- Per aderire e' necessario avere un IdP nella Federazione IDEM

In ogni caso questo tipo di configurazione dei client richiede un minimo di intervento da parte dell'utente e non e' automatico

Username/password

- RADIUS puo' essere configurato per gestire gli utenti e password, insieme ad alcuni attributi, tipo il realm dell'utente
- Zeroshell ha una interfaccia semplice di gestione degli utenti/password e di popolamento del RADIUS
- RADIUS potrebbe essere configurato aggiungendo il modulo LDAP per andare a pescare la coppia utente/password su LDAP istituzionale --- ma e' sconsigliato
- Conviene tenersi un DB locale e gestire gli utenti che fanno richiesta di accesso wireless a parte
- Questa soluzione e' utile per produrre account di accesso temporaneo o in occasione di eventi e convegni

NB: Questa configurazione e' molto simile ad eduroam, e zeroshell puo' essere utilizzato: basta configurare il RADIUS di zeroshell come proxy verso quello di gerarchia superiore

Router o Bridge

Zeroshell puo' funzionare sia in modalita' bridge che router

- Nella modalita' bridge funziona solo come captive-portal e autenticatore
- Nella funzione router fornisce anche servizi di DHCP e DNS, oltre al NAT e al routing
- Dalle ultime versioni puo' svolgere le due funzioni contemporaeamtente, funzionando da router per certe sottoreti e da bridge per altre

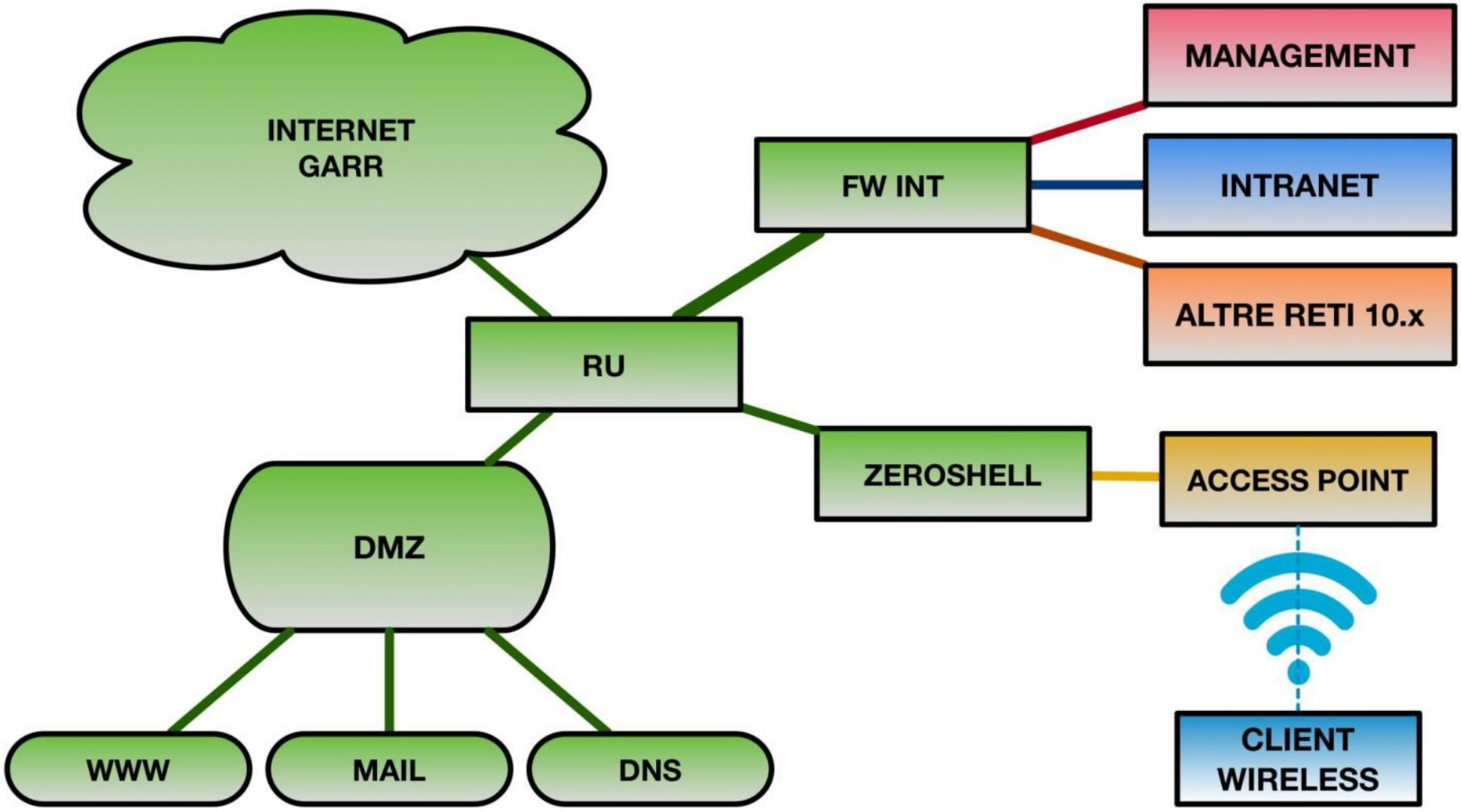
Nel caso della nostra piccola rete wireless conviene delegargli tutta la gestione facendogli fare NAT, DHCP DNS (forwarder verso quello istituzionale)

Considerazioni Topologiche

La rete wireless e' ostile

- Attacchiamo l'iterfaccia esterna di zeroshell direttamente al nostro router di bordo
- Oppure allo switch della DMZ
- L'interfaccia interna dovra' far parte della rete degli accesspoint che avra' indirizzi pri
- Cosi' sono nel punto piu' lontano dalla rete interna
- Ovviamente ogni accesso alla rete interna, di qualsiasi tipo e' interdetto
- Se un ospite ha necessita' di utilizzare con la wireless servizi interni non puo' farlo o usare un altro sistema
- Se volessimo dare servizi di stampa ad untenti wireless valutare l'installazione di una stampante anche scarsa, in DMZ

Schema


INTERNET
GARR
MANAGEMENT
FW INT
INTRANET
ALTRE RETI 10.x
RU
ZEROSHELL
ACCESS POINT
DMZ
WWW
MAIL
DNS
CLIENT
WIRELESS

SERVIZI DI STAMPA

Servizi di stampa

Policy univoca per la stampa

- Una stampante «privata» per PC dipendente?
- Una o piu' stampanti di rete accessibili da tutti?
- O da classi di utenti diverse?

  Es. I dipendenti che potrebbero stampare documenti particolari usano una stampante solo per loro in una stanza apposita

Esempio Cups + samba

Mettere in intranet un server cups

- con un piccolo samba
  - Tutto chiuso
  - Contiene solo la parte [printers]

Configurare su cups eventuali ACL su stampanti (chi puo' fare cosa)

Abilitare il forward verso la intranet TCP/631

(e forse anche samba) per ogni IP o rete INTERNA che puo' stampare:

```
iptables –A FORWARD –i eth2 –s 10.2.0.0/16 –o eth1 –d ip.del.server.stampa –dport 631
```

Considerazioni di sicurezza

Non si puo' stampare sul server di stampa dalla rete UNTRUSTED!!!

- La DMZ
  - Non dovrebbe avere client che stampano, ma solo server
- Gli utenti wifi
  - Generalmente non hanno bisogno e forse neanche diritto a stampare
  - Altrimenti prevedere una stampantina in DMZ

Oppure gli utenti wifi per stampare usano la VPN

- Configurare il forward sulla TCP/631 anche dalla rete VPN (v. oltre)

  NB: e' sconsigliato perche' apre una breccia sulla intranet

Le stampanti

Solitamente hanno firmware linux

- Vecchissimo... Degli anni 90. Obsoleto ... Non patchato
- Per ogni problema il vendor impiega molto tempo a correggere
- Difficile la gestione di una policy di aggiornamento firmware

Configurare staticamente gli IP della stampante

Entrare nel pannello di gestione e disabilitare tutto: NTP, SNMP, TFTP, small TCP services

Devono solo avere un IP e LPD...

Devono solo stampare!!!

IoT

Dispositivi IoT

Sonde, dispositivi di vigilanza, IoT, stampanti stesse

Anche in questo caso spesso hanno installato firmware linux vecchio e neanche piu' supportato

Prima di tutto vanno configurate per svolgere solamente il lavoro che devono fare

Dovrebbero stare nella stessa sottorete dei propri utilizzatori

- Es. Sonde di esperimenti – rete del proprio laboratorio

Sonde di monitoraggio

Si intende monitoraggio di temperatura di un ambiente, o monitoraggio del lavoro di una macchina o di un acceleratore di particelle... Qualsiasi tipo di sonda consultabile dalla rete

- Valutare il firmware degli oggetti
- Chiudere tutto quello che non serve
- Valutare il rischio
- Stabilire chi puo' accedere
- Decidere se metterli in un segmento a parte (consigliato)
- In ogni caso non mettere mai sonde in DMZ

Videosorveglianza

Stesso procedimento per le sonde di monitoraggio ma il rischio e' maggiore perche' i dati sono piu' importanti

Inoltre

- Troppe vulnerabilita' firmware non documentate
- Mancato rilascio patch dai costruttori

Potrebbero essere messe in intranet (se accedono i dipendenti o servizi esterni di vigilanza)

- *Valutare se metterli in una rete fisicamente a parte, non raggiungibile se non da una postazione fisica*
- Nel caso che debbano essere acceduti da remoto creare una VPN apposita non ruotata e accedibile solo tramite VPN

VPN

VPN

Una **VPN** (Virtual Private Network) e' un sistema di incapsulamento dei pacchetti per collegare fra se' sedi remote come se fossero collegate sullo stesso cavo fisico

Anche se nel mezzo devono attraversare tutta internet

E' di diversi tipi, con diversi protocolli... principalmente:

- **PPTP**: permette ad un PC di connettersi direttamente ad un altro PC o server
- **LAN-LAN**: permette di collegare fra se' sedi distaccate di enti come se fossero collegate sullo stesso segmento fisico
- **Host-LAN**: permettono di connettere singoli PC client in una LAN locale

Tutto questo puo' essere fatto con diversi protocolli, nel caso piu' semplice viene fatto attraverso un tunnel SSL/TLS

Valutare bene l'effettivo bisogno di aprire brecce sulla intranet

Come funziona

Il server sta in ascolto sulla porta UDP/1194

Il client si connette a quella porta

Verifica il certificato SSL del server e viceversa e inizia la comunicazione via SSL

Viene stabilito il protocollo

Viene chiesta l'autenticazione dell'utente

- Tramite certificato digitale X.509

Verificata l'identita' il client e il server stabiliscono una fra di se' un tunnel SSL

Da questo momento in poi ogni comunicazione verra' criptata attraverso internet ed il client si trova seduto "sul server VPN"

Quindi?

Il compito di una VPN e' potenzialmente finito, il tunnel e' stabilito: il client raggiunge il server

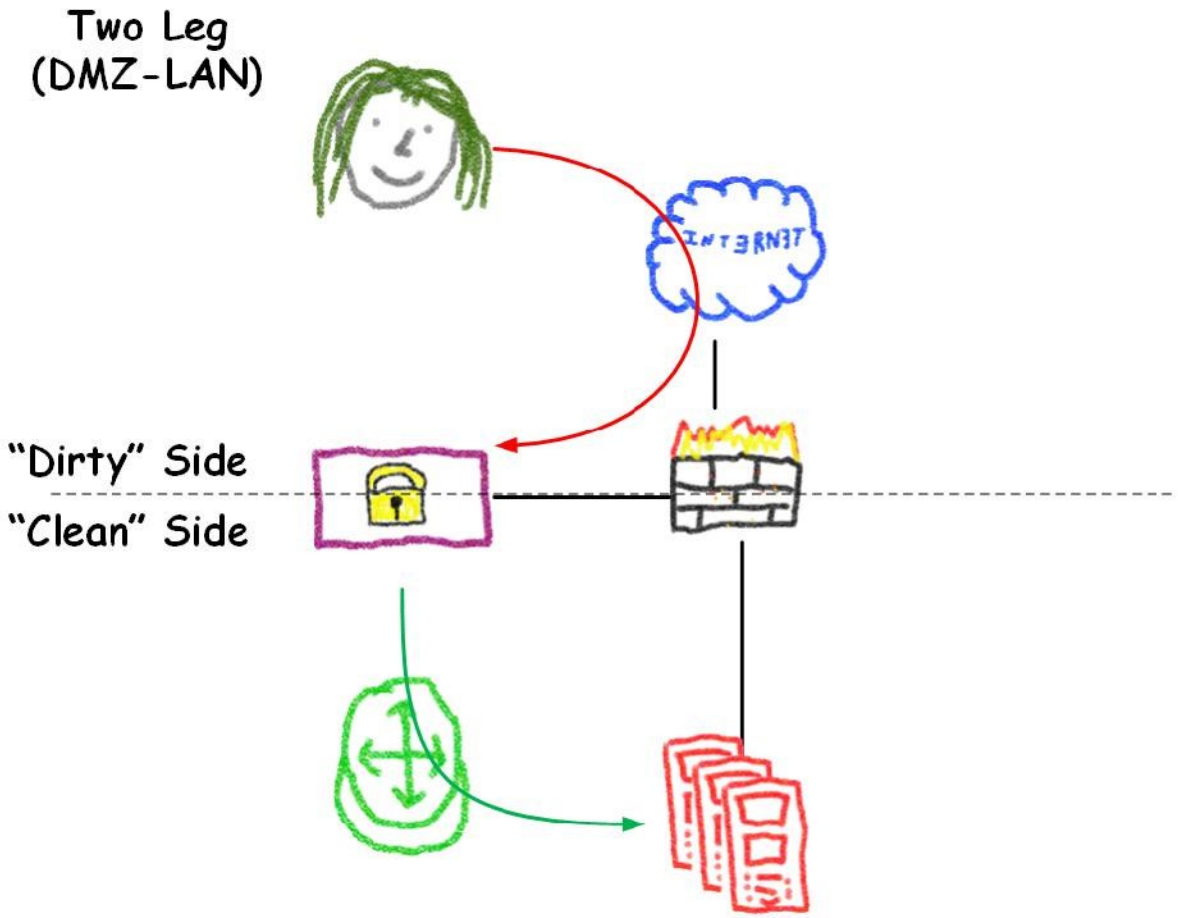
A questo punto vogliamo che il client si possa collegare alla nostra intranet

Dobbiamo assegnargli un indirizzo IP e le rotte necessarie e il DNS

Per fortuna gran parte dei software di VPN possono essere configurati per farlo da soli

Architettura proposta: 2 LEG routing VPN

Il firewall verde in figura e' il VPN stesso mediante iptables



Come implementare una VPN

Architettura a 2 legs (DMZ-DMZ) che e' quello ritenuto ragionevolmente piu' sicuro per una rete di piccole dimensioni

- Ai client, dopo l'autenticazione col certificato personale, viene assegnata una rete interna diversa dalle altre (10.8.0.0/16)
- Ai client viene assegnato un IP statico a seconda dell'utente che si connette
  - Tipo: Mario Rossi, che si autentica col certificato CN=Rossi, avra' IP 10.8.0.10
- Ai client viene infine passata la rotta statica e il DNS da interrogare
  - Default gw 10.8.1.1, DNS 192.84.145.20

VPN routing

Nella configurazione proposta il server VPN fa anche da router/firewall per la rete 10.8 degli utenti remoti

Questo aggiunge un livello di sicurezza in piu' dato che VPN ha due interfacce

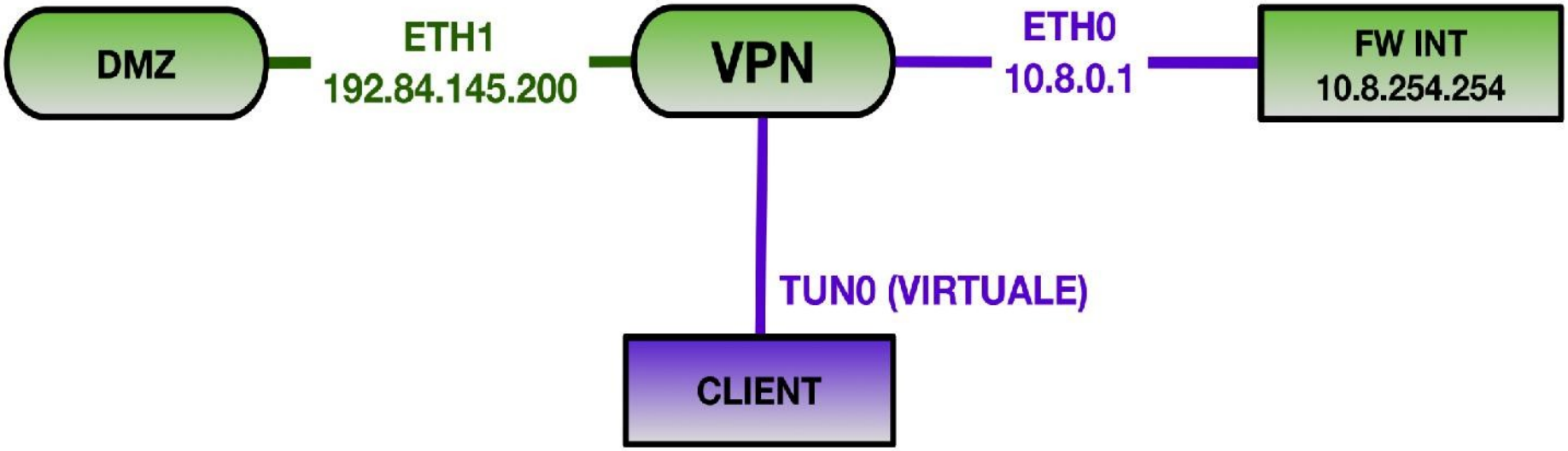
- una collegata in DMZ, per essere raggiunto dagli utenti remoti
- Una collegata all'interno della LAN su fw interno

In questo modo diamo ai client come default gw l'interfaccia verso fw-int del VPN

Configuriamo dei filtri restrittivi in entrata e in uscita su entrambe le interfacce di VPN

Segmentazione all'ennesima potenza!

Schema


DMZ
ETH1
192.84.145.200
VPN
ETH0
10.8.0.1
FW INT
10.8.254.254
TUN0 (VIRTUALE)
CLIENT

Hardening VPN server

Ascolta su TCP invece che il default UDP

proto tcp

Routed/firewalled VPN

dev tun

server 10.8.0.1 255.255.0.0

push "route 10.8.0.0 255.255.0.0"

Assegno indirizzi IP statici (per poi scrivere le regole di accesso sul firewall)

client-config-dir ccd

Creo un file ccd/Rossi (come il CN) e ci metto il suo IP:

ifconfig-push 10.8.0.50 10.8.0.1

Configurazione VPN client

Diciamo che siamo un client

client

Usiamo la stessa interfaccia e protocolo del server

dev tun

proto tcp

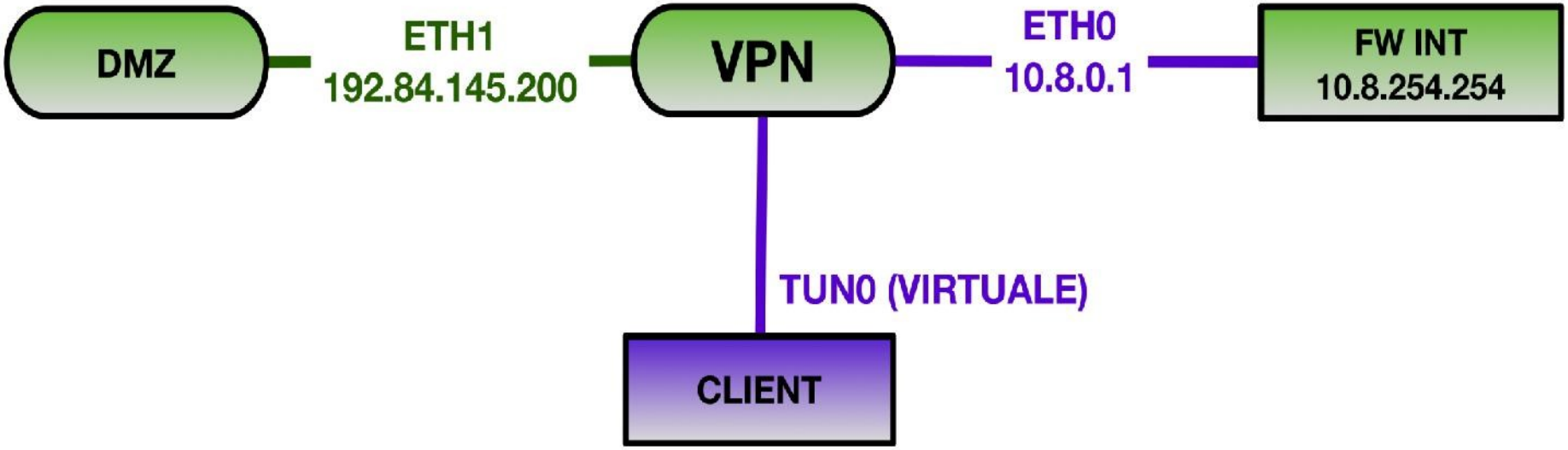
Indichiamo il server

remote-server vpn.uniXX.it 1194

Verifica del certificato server

remote-cert-tls server

Ricordiamoci lo schema



Configurazione del routing

Su VPN vanno inserite regole restrittive per i client che entrano in VPN

Ulteriori controlli verranno fatti poi da fw-int

1. Impedire che pacchetti escano dall'interfaccia verso la DMZ (tranne gli ESTABLISHED ovviamente)
2. Impedire il FORWARD verso l'interfaccia della DMZ
3. Consentire l'uscita degli IP sulla LAN soltanto verso la loro destinazione assegnata (Es. Se Rossi puo' usare solo la procedura stipendi e' necessario scrivere la regola piu' restrittiva possibile per limitare il suo traffico

Firewalling e routing su server VPN

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A INPUT -p udp --dport 1194 -m state --state NEW -s 0.0.0.0/0 -j ACCEPT

iptables -I OUTPUT 1 -m state --state RELATED,ESTABLISHED -j ACCEPT

iptables -A INPUT -i tun0 -j ACCEPT

iptables -A FORWARD -m conntrack –ctstate RELATED,ESTABLISHED -j ACCEPT

iptables -A FORWARD -i tun0 -o eth1 -j DROP

iptables -A FORWARD -i eth0 -o eth1 -j DROP

iptables -A FORWARD -i eth1 -o eth0 -j DROP

iptables -A FORWARD -i tun0 -s 10.8.0.0/16 -d 10.8.0.0/16 -j DROP
```

Note

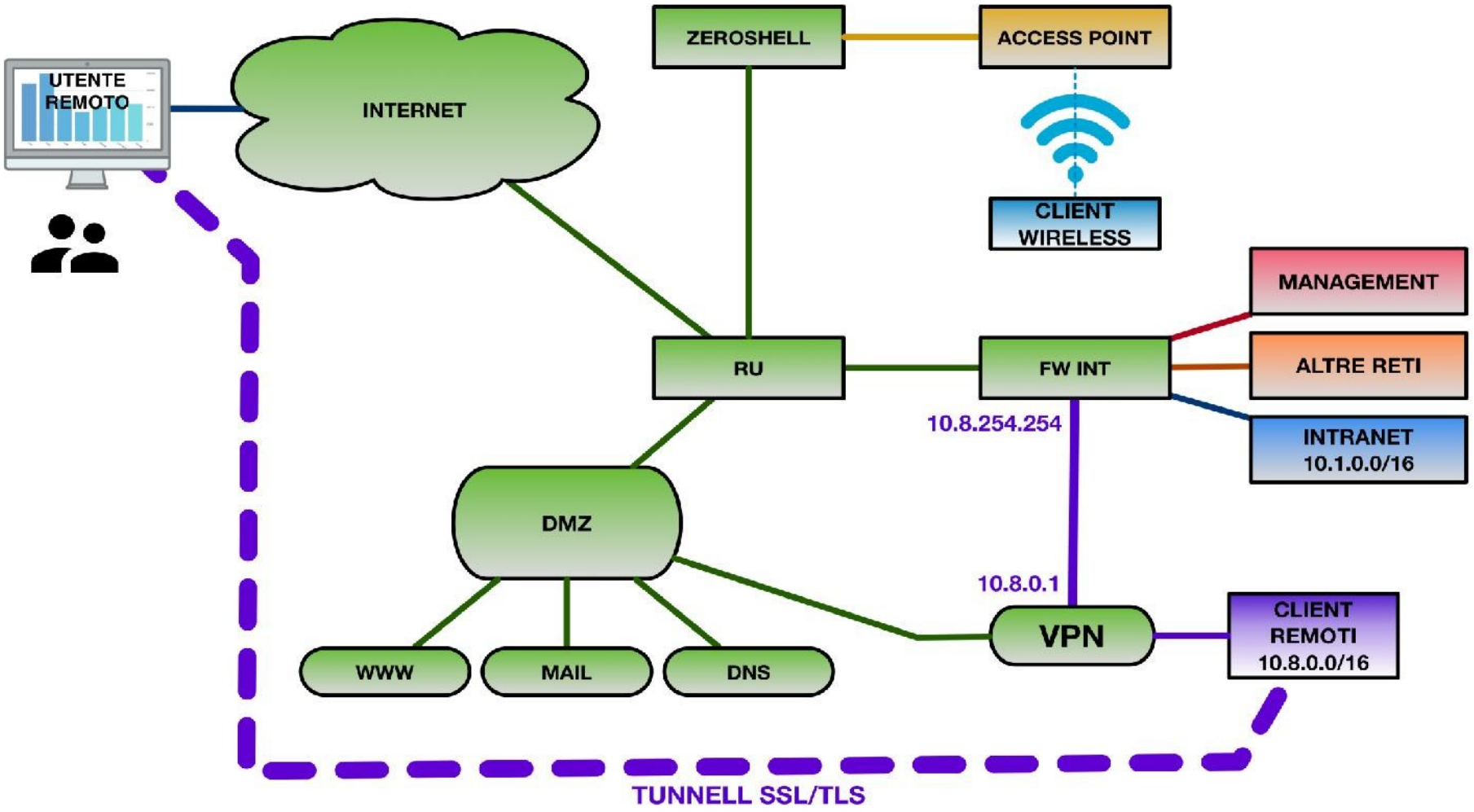
Per installare una VPN e’ necessario avere certificati personali e server

Se si ha una CA fatta in casa deve essere resa trusted

Si possono usare i certificati TERENA

Si puo’ semplificare utilizzando una autenticazione solo LDAP (ma non e’ standard)

La mia rete


UTENTE REMOTO
INTERNET
ZEROSHELL
ACCESS POINT
CLIENT WIRELESS
MANAGEMENT
ALTRE RETI
INTRANET 10.1.0.0/16
RU
FW INT
10.8.254.254
DMZ
10.8.0.1
VPN
CLIENT REMOTI 10.8.0.0/16
WWW
MAIL
DNS
TUNNELL SSL/TLS

HARDENING

Harden yourself

La prima cosa su cui fare hardening e' ***se stessi e l'utente***

- Politica delle password
  - LUNGHE
  - A validita' limitata – forzare il cambio
  - Evitare il riutilizzo
- Non cliccare a caso
  - Link su pagine web
  - Link su mail
- Riconoscere un mail di SPAM
- Non installare applicazioni craccate o di dubbia provenienza

HARDENING LINUX

Hardening Linux

In rete ci sono migliaia di checklist aggiornate su come hardenizzare una macchina linux

Ci sono anche specifiche per distribuzione...

Sistema

- Registrare IP, nome, MAC address, referente, numero di inventario, software installato (vale anche per windows)
- Protezione del BIOS
- Criptazione del disco
- Partizioni separate, soprattutto /tmp

Sistemi Linux - hardening del Sistema

Montare la /tmp come nodev,nosuid,noexec

Tenere /boot readonly (in fstab)

Password al GRUB

Tenere il sistema aggiornato

Limitare la grossezza dei coredump

Configurare syslog remoto

Limitare i permessi a tutte le director cron e at

Configurare l'exec shield e randommizzare l'utilizzo della memoria virtuale

Sistemi Linux - Hardening della Rete

Rete

Eliminare i servizi legacy (telnet, xinetd, identid)

Disabilitare tutti i servizi che non servono

Configurare iptables locale per se' stesso

- Disabilitare ip.forwarding, «send packet redirect», source routed packet, ICMP redirect
- Abilitare Ignore Broadcast Request, Bad Error Message Protection, TCP/SYN cookies

Linux - Monitoraggio

Utilizzare strumenti di monitoraggio che spediscano i log al log server per scovare eventuali problemi

Sichiamano HIDS (Host Intrusion Detection System)

- OSSEC
- Snort
- Suricata
- Nagios

HARDENING WINDOWS

Soluzioni

I signori di Microsoft consigliano:

- Configurare User Account Control
- Abilitare SecureBoot
- BitLocker
- Defender firewall per bloccare tutto il traffico
- Installare l'estensione uBlock Origin sui browser Chrome e Edge
- Patchare sempre
- Hypervisor Code Integrity (nuova feature)

Hardening software

Per fortuna ci sono dei programmi che cercano di farlo in automatico – consigliatissimi

Windows-10-Hardening

An admittedly frivolous (and infrequently updated) attempt to harden Windows 10.

https://github.com/aghorler/Windows-10-Hardening

SysHardener

This free security tool helps you harden Windows settings to mitigate online threats

https://www.wilderssecurity.com/threads/syshardener-harden-windows-settings.401092/

Antivirus

Il malware e' sempre diverso

Viene distribuito come sorgente – modificabile

- Es. MIRAI botnet

Gli antivirus basati su firme non riescono a tenere traccia di tutto, solo circa del 40-50%

Sono diventati poco efficienti

Endpoint Detection and Response

Gli EDR (endpoint detection and response) sono sistemi che funzionano tramite baseline

Hanno nel loro «DB» la baseline completa di una macchina windows

- Chiamate al kernel
- DLL utilizzate
- Connessioni stabilite

Per ogni eseguibile di sistema e i piu' importanti applicativi utilizzati (qualcuno arriva a 3000 applicativi conosciuti)

EDR

Il sistema manda allarmi quando la macchina inizia a fare qualsiasi cosa fuori dalla propria baseline

Non e' basato su quello che fa l'utente, ma su quello che fanno le applicazioni per funzionare

Va affiancato al software antivirus, che comunque non va eliminato

L'ultima volta che ho studiato l'argomento non c'erano ancora prodotti Free o OpenSource purtroppo

Monitoraggio host

Gli HIDS per windows

Anche in questo caso i log dovrebbero essere gestiti dal syslog remoto, cosi' aggiungono informazioni sulla nostra rete per ElasticSearch

- OSSEC
- Snort
- Suricata

HARDENING SERVIZI

apache

Farlo correre come utente non privilegiato

Disabilitare tutti i moduli che non servono

Configurare tutto in SSL, eliminare HTTP!!!

Evitare di dare informazioni sul server

- ServerTokens Prod
- ServerSignature Off
- Header always unset X-Powered-By
- TraceEnable Off

Controllare I permessi sui file

apache

Il rischio di compromissione attraverso apache non e' tanto dovuto al server web in se'

Sono le applicazioni (php, java, js) che introducono problemi e falle (SQLi)

Bisogna stare attenti a come vengono programmate le applicazioni

- Sanificare l'input
- Controlli sui tipi di dati in input
- Controlli sui caratteri speciali in input
- Escape delle stringhe

ssh

NB: ssh non serve sempre. Disabilitarlo se non si usa!

PermitRootLogin no

AllowUsers [username]

IgnoreRhosts yes

HostbasedAuthentication no

PermitEmptyPasswords no

X11Forwarding no

MaxAuthTries 5

Ciphers aes128-ctr,aes192-ctr,aes256-ctr

UsePAM yes

ClientAliveInterval 900

ClientAliveCountMax 0

Domande?

Grazie!