Università degli Studi di Camerino

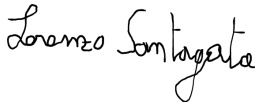
Scuola di Scienze e Tecnologie

Corso di Laurea in Informatica (Classe L-31)

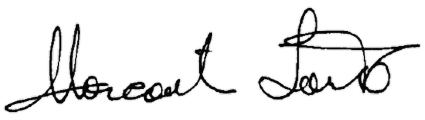
Captive Portal con Active Directory. Caso di studio: una rete scolastica.

Laureando
Lorenzo Santagata

Matricola 105369



Relatore
Prof. Fausto Marcantoni



A.A. 2020/2021

Indice

1. Abstract

Questa tesi vuole descrivere un caso di studio reale riguardante la configurazione di una rete scolastica.

In questo ambiente abbiamo infatti diverse problematiche da risolvere come l'autenticazione degli studenti e dei docenti, la creazione di policy diverse a seconda del tipo di utente e così via.

Si utilizzeranno per i nostri scopi il firewall Pfsense che permette di creare un captive portal per l'autenticazione degli utenti con active directory che verrà installato sul server Windows.

Verrà fornita una guida completa all'installazione e configurazione di tutto il nostro sistema.

Nella sezione 1.3 illustreremo la struttura della tesi e gli argomenti che andremo a trattare.

1.1 Motivazione

Le motivazioni che mi hanno spinto alla stesura di questa tesi sono diverse, anzitutto la mia volontà di approfondire una tematica riguardante le reti e il mio crescente interesse per la sicurezza informatica, soprattutto dopo aver avuto la possibilità di partecipare al progetto della CyberChallenge 2021.

1.2 Obiettivi

La tesi si porrà l'obiettivo di approfondire e spiegare i seguenti aspetti:

- Fornire una comprensione generale di cosa sia un firewall
- Illustrare i principali pregi e difetti di un Firewall
- Descrivere le problematiche relative al caso di studio.
- Descrivere nel dettaglio come si è fatto per soddisfare le problematiche della rete scolastica del caso d'uso.

Verranno analizzate le tecnologie e i software utilizzati per studiare il comportamento di una rete scolastica

1.3 Struttura della Tesi

La tesi è strutturata nel seguente modo:

- Introduzione alla virtualizzazione
- Firewall
- Pfsense
- Windows Server
- Caso di studio una rete scolastica

Nella prima sezione si farà un'introduzione della virtualizzazione e si forniranno i rudimenti di questa tecnologia.

Nei capitoli inerenti al firewall si fornirà una descrizione di queste soluzioni e si elencheranno i pregi e i difetti. Si farà anche un confronto tra le principali differenze tra firewall commerciali e opensource.

Si descriveranno nel seguito di Pfsense e Windows Server elencando le funzioni utilizzate e fornendo una breve guida all'installazione

Nella parte finale si entrerà nei dettagli analizzando il caso di studio fornendone una descrizione, una guida all'installazione e una configurazione dei software utilizzati.

2. Introduzione

In questa sezione verrà affrontato il tema della virtualizzazione perché questa tecnologia verrà utilizzata molto all'interno della tesi per installare Pfsense, windows server e le macchine degli studenti e i docenti.

2.1 Breve introduzione alla virtualizzazione

La virtualizzazione è una tecnica che permette di astrarre le componenti hardware. Grazie a questa capacità è possibile installare sistemi operativi su hardware virtuale. [Wiki]

Spesso si viene a creare una confusione tra le definizioni di virtualizzazione simulazione ed emulazione.

Nella simulazione si ha la replica di un sistema per mezzo del software. Sono riprodotte le componenti del sistema, la loro logica le funzioni nell'interazione con altri sistemi.

Un utilizzo pratico dei simulatori si ha quando si vogliono compilare programmi, per finalità di analisi, che sono stati sviluppati per un altro particolare sistema.

Un esempio consiste nella simulazione su computer moderni di software che era stato progettato per dei calcolatori oramai in disuso.

L'emulazione invece copia le funzioni delle componenti hardware o software ma non la loro logica. Il fine dell'emulazione è quello di ottenere con il sistema riprodotto gli stessi risultati che ottiene l'hardware reale. L'emulatore può quindi sostituire completamente i sistemi che riproduce. [ion06]

Riassumendo la virtualizzazione è quindi una tecnica che differisce da quelle dell'emulazione o della simulazione.

2.2 Virtualizzazione di hardware

Nella tesi si utilizzerà la tecnica della virtualizzazione dell'hardware.

Questa tecnica ci permette di creare una macchina virtuale che si comporta per l'utente finale allo stesso modo di un computer fisico dotato di hardware e sistema operativo. Queste macchine funzionano come sistemi guest virtuali su uno o più sistemi fisici detti **host**.

La virtualizzazione dell'hardware è quindi una tecnica relativamente sicura contro eventuali Hacker. Infatti, ogni sistema guest è eseguito, in modo isolato, in un ambiente hardware virtuale. Se uno dei sistemi guest viene attaccato da hacker o danneggiato

da un malware nelle sue funzioni, ciò non ha di solito ripercussioni sugli altri sistemi guest e sul sistema host che le ospita.

Una reale minaccia è però rappresentata dagli attacchi in cui gli hacker sfruttano le vulnerabilità del software hypervisor per riuscire ad avere accesso al sistema host sottostante. [ion06]

Possiamo riassumere nella tabella i vantaggi e gli svantaggi di questa tecnica.

Vantaggi	Svantaggi
Possibilità di installare uno o più sistemi operativi guest su hardware virtuale.	La performance di una macchina virtuale può essere influenzata da altre macchine virtuali attive sullo stesso sistema host
Le macchine virtuali offrono un livello di isolamento e conseguentemente di sicurezza relativamente alto.	Problemi di sicurezza legati agli attacchi Hacker all' hypervisor sottostante

Tabella 2.1: Virtualizzazione pro e contro [ion06]

2.3 Hypervisor

Un hypervisor detto anche Virtual Machine Monitor è un software che consente il funzionamento di più sistemi guest su un unico host. L' hypervisor gestisce le risorse hardware messe a disposizione dal sistema host, come ad esempio CPU, RAM, memoria di archiviazione e periferiche e le condivide con tutti i sistemi guest che sono installati sull'host.

Con la virtualizzazione viene riprodotto dall'hypervisor di ciascuna macchina virtuale un ambiente hardware completo. In questo modo ogni macchina dispone delle proprie risorse hardware che sono indipendenti da quelle degli altri sistemi guest. Mentre l'hardware fisico del sistema host rimane nascosto al sistema operativo guest. Le soluzioni software più popolari per la virtualizzazione sono Oracle VM VirtualBox, VMware Workstation e Microsoft Hyper-V.[ion06]

In questa tesi viene utilizzato VirtualBox che è un software gratuito e open source.

Link VirtualBox: https://www.virtualbox.org/wiki/Downloads

3. Firewall

In questa sezione del documento verrà descritto che cos'è un firewall e verranno analizzati i vantaggi e gli svantaggi che esso comporta. Verrà inoltre fornito un elenco dei principali firewall commerciali e opensource.

3.1 Cos'è il Firewall

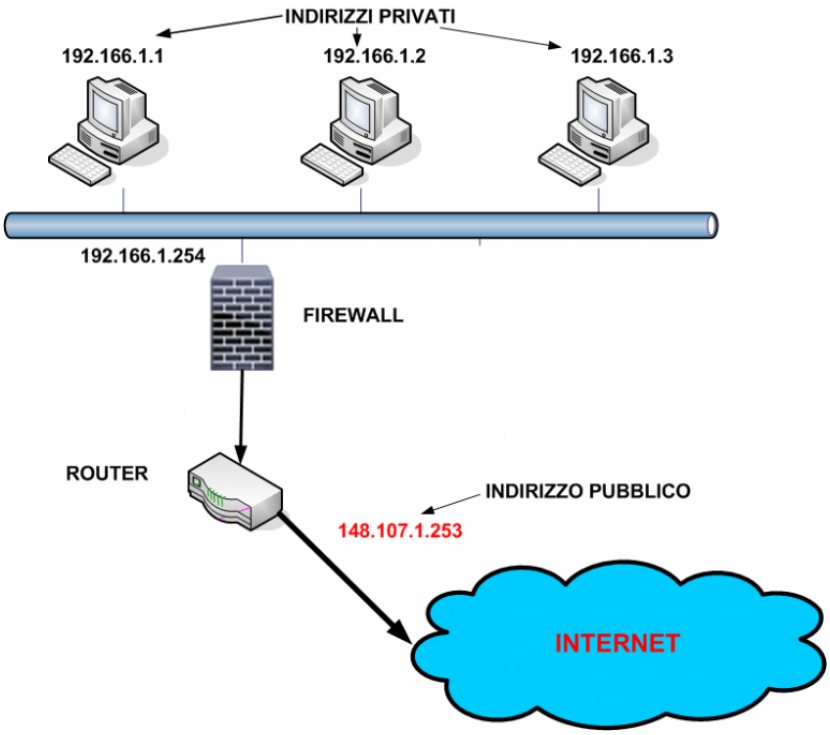


Figura 3.1: Firewall [AS]

Un firewall è un dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare i pacchetti in transito.

Esso può essere una componente hardware o un software che si trova direttamente installato su un pc o server.

Il firewall si interpone tra la sottorete interna locale ovvero la LAN che comprende i dispositivi locali e la rete esterna che si collega ad internet. Questo fa sì che la rete LAN sia isolata e non accessibile dalla rete esterna.

Per questo motivo può essere utile creare una sottorete chiamata zona demilitarizzata o DMZ che andrà a contenere quei servizi che devono essere isolati dalla rete interna ma che devono essere protetti dal firewall e raggiungibili dall'esterno. [Wikd] [Cis]

3.2 Tipi di Firewall

Esistono diverse tipologie di firewall che sono state sviluppate nel corso degli anni e queste comprendono:

- Firewall packet filter o stateless firewall
- Firewall stateful inspection
- Firewall proxy
- Next-Generation Firewall

Firewall packet filter o stateless firewall

Questo firewall è stato il primo ad essere ideato. Esso si basa sull'analisi di ogni pacchetto che la attraversa senza tenere conto dei pacchetti precedenti. Infatti, viene detto anche stateless firewall o firewall senza memoria di stato.

Durante l'analisi del pacchetto vengono analizzate solo le informazioni contenute nell'header e in modo particolare quelle appartenenti ai primi tre livelli del modello Osi e alcuni elementi del livello quattro. Le informazioni che vengono analizzate sono l'indirizzo IP della sorgente, l'indirizzo IP della destinazione, la porta della sorgente, la porta della destinazione e il protocollo di trasporto. Le regole o policy del firewall impostate dall'amministratore di rete stabiliscono quali pacchetti possono passare e quali devo essere bloccati, prendendo in considerazione i dati dei pacchetti che vengono analizzati. Pochi firewall di questa generazione supportano funzionalità come il logging e il reporting. Questo firewall risulta vulnerabile ad attacchi di tipo IP spoofing in quanto non avendo la memoria di stato non può sapere se un pacchetto appartiene ad una connessione ancora attiva oppure no. Quindi un pacchetto malformato da un attaccante con un IP sorgente che viene modificato con uno consentito dalle policy del firewall viene lasciato passare. Inoltre, questo tipo di firewall filtrando solo le informazioni dei livelli più bassi del modello OSI non permette di prevenire attacchi che si basano su vulnerabilità dei livelli superiori. [Wikd]

Vantaggi	Svantaggi
Filtrare il traffico e scartare i pacchetti che non rispettano le policy o regole del firewall	Vulnerabile ad attacchi di tipo Ip spoofing

Tabella 3.1: Firewall stateless pro e contro

Firewall Stateful Inspection

Il firewall Stateful Inspection consente o blocca il traffico secondo regole basate sullo stato, sulle porte e sul protocollo. Monitora tutta l'attività dal momento in cui viene

stabilita una connessione fino alla sua chiusura. L'applicazione del filtro viene decisa sulla base delle regole definite dall'amministratore e dalle informazioni raccolte dai pacchetti, ovvero quelle relative a connessioni precedenti e pacchetti appartenenti alla stessa connessione.

Esso aggiunge rispetto al firewall stateless la capacità di mantenere lo stato della connessione TCP e grazie a questa caratteristica determina se bloccare o consentire il passaggio di un pacchetto. Questa funzionalità, detta stateful inspection, viene implementata utilizzando una tabella dello stato.

Infatti, le connessioni TCP in corso vengono memorizzate in una tabella di connessione interna al firewall nella quale ognuna di esse viene rappresentata da due coppie formate da indirizzo IP e porta, una per ciascun endpoint della comunicazione.

Questo è possibile perché il firewall è in grado di osservare sulla rete l'inizio di una nuova connessione TCP, considerando i pacchetti che hanno i flag SYN SYNACK e ACK e la fine della stessa, ovvero quando vede un pacchetto con flag FIN per quella connessione. Si tiene traccia anche del sequence number e dell'acknowledgement number dei pacchetti. Il firewall può anche assumere che la connessione sia terminata quando non vede alcuna attività su di essa in un periodo determinato di tempo.

In generale, rispetto ai stateless firewall, offrono una maggiore sicurezza, un logging migliore e un controllo migliore sui protocolli applicativi che scelgono casualmente la porta di comunicazione come ad esempio FTP, ma sono meno performanti di un firewall stateless e le regole da impostare per il filtraggio risultano più complesse di quelle di un firewall stateless.

Questa tipologia di firewall protegge dagli attacchi di tipo IP spoofing visto che mantiene lo stato della connessione, ma è vulnerabile ad attacchi di tipo DoS in particolare il session table flood attack dove la tabella dello stato viene "inondata" di dati fino a riempirla, in modo da non poter effettuare più nuove connessioni. [Junno]

Inoltre, gli statefull firewall non rilevano attacchi nei livelli superiori al quattro del modello OSI. [Wikd]

Vantaggi	Svantaggi
Maggiore sicurezza, un logging migliore e un controllo migliore sui protocolli applicativi che scelgono casualmente la porta di comunicazione come ad esempio FTP	Meno performanti di un firewall stateless e le regole da impostare per il filtraggio risultano più complesse di quelle di un firewall stateless.
Questa tipologia di firewall protegge dagli attacchi di tipo IP spoofing visto che mantiene lo stato della connessione	Vulnerabili ad attacchi di tipo DoS session table flood attack.

Tabella 3.2: Firewall stateful pro e contro

Firewall proxy

Un application firewall o proxy firewall o application gateway opera fino al livello sette del modello OSI filtrando tutto il traffico di una **singola applicazione** sulla base della conoscenza del suo protocollo. Questo tipo di firewall esegue una deep packet inspection o analisi profonda del pacchetto considerando quindi non solo l'header ma

anche il contenuto (payload) dello stesso ed è quindi in grado di distinguere il traffico di un'applicazione indipendentemente dalla porta di comunicazione che questa utilizza. Un'altra caratteristica che lo distingue da un stateless firewall e da uno stateful firewall è la capacità di fare da gateway per la connessione tra un host della rete interna che protegge e un altro host della rete esterna. Quindi in una connessione questo firewall è l'unico elemento che interagisce con l'esterno, nascondendo così gli host della rete locale.

Questo tipo di firewall è in grado di rilevare i tentativi di intrusione e di realizzare le funzionalità di logging e reporting in modo migliore rispetto ai firewall di vecchia generazione. Sebbene aumenti il livello della sicurezza, un application firewall è specifico per ogni applicazione e costituisce un collo di bottiglia per le performance della rete introducendo ritardi e rallentamenti. Inoltre, si crea un problema per la privacy visto che viene analizzato il payload e non solo l'header come nei firewall precedenti.[Wikd] [And14] [Wikb]

Vantaggi	Svantaggi
Filtraggio fino al livello sette per una singola applicazione	Bisogno di creare più firewall per ogni singola applicazione
Maggiore sicurezza e protezione	Essendo specifico per ogni applicazione crea un problema di prestazioni

Tabella 3.3: Firewall proxy pro e contro

Next-Generation Firewall

Un next-generation firewall è uno strumento che riunisce diverse tecnologie per la sicurezza come quelle per il filtraggio dei pacchetti delle generazioni precedenti di firewall come il filtraggio stateless ma anche la stateful inspection dei firewall Stateful e l'analisi dei pacchetti a livello applicativo (deep packet inspection). Rispetto ai precedenti firewall questo aggiunge il supporto alla VPN e al Nat, oltre al rilevamento e la prevenzione delle intrusioni (sistemi IDS e IPS) e la definizione di policy specifiche per ogni applicazione.

Questa tipologia di firewall ha come scopo quello di rendere molto più semplice l'utilizzo di strumenti, molto diversi tra loro, per migliorare la sicurezza dei sistemi sui quali vengono installati.

Il Next-Generation Firewall protegge dagli attacchi fino al livello sette del modello OSI. [Wikd] [RK17] [Cis]

Essendo uno strumento molto completo e garantendo maggiore sicurezza rispetto alle precedenti generazioni di firewall, si può incorrere in problemi relativi all'accesso da remoto. Ad esempio in Australia con la maggior parte dei lavoratori che si sono trovati a lavorare in smart working, si sono creati dei problemi per gli impiegati che provavano ad accedere alla VPN aziendale da casa, in quanto il firewall negava loro l'accesso perché non riteneva la rete sicura.[IT g]

Vantaggi	Svantaggi
Raggruppare più tool per la sicurezza in un unico strumento	Difficoltà ad accedere ai server aziendali in caso di lavoro remoto
Unire più strumenti per la sicurezza in uno solo porta una riduzione dei costi di mantenimento e aggiornamento.	

Tabella 3.4: Next Generation Firewall pro e contro

3.3 Vantaggi nell'uso del Firewall

Come abbiamo visto, il vantaggio principale e più importante di un firewall è la protezione dalle minacce esterne. Filtrare il traffico permette all'amministratore di rete di creare delle regole in modo tale da bloccare il traffico indesiderato o potenzialmente pericoloso.

Inoltre, i sistemi firewall più avanzati ci permettono di proteggerci da attacchi informatici, che senza uno strumento come questo a protezione della nostra rete avrebbero successo.

Di seguito possiamo vedere molti dei vantaggi che l'utilizzo di un firewall ci fornisce:

- Filtrare e bloccare pacchetti che non rispettano le policy del firewall

  Come abbiamo visto precedentemente attraverso le regole impostate dall'amministratore di sistema, il firewall può bloccare dei determinati tipi di pacchetti o consentire ad altri di passare. Ad esempio, un'organizzazione che non voglia che si possa dall'esterno creare una mappa della propria rete interna, tramite Traceroute, può bloccare tutti i messaggi ICMP con TTL esaurito che lasciano la rete dell'azienda. [RK17]

- Blocco contenuti non pertinenti

  Con un firewall si possono bloccare determinati siti o la connessione a determinate porte in base a un criterio riguardante non tanto la sicurezza ma le politiche di una data società.

  Si potrebbero quindi bloccare i contenuti non pertinenti con l'attività lavorativa, o in ambiente domestico i contenuti non adatti ai minori.

- Scartare i pacchetti malformati inviati dagli attaccanti

  Come detto precedentemente nel caso di stateful firewall possiamo controllare lo stato delle connessioni tcp tramite la tabella di connessioni, questa caratteristica è molto utile per prevenire bloccare la recezione di pacchetti malformati(spoofed) da parte di un attaccante. Ci basterà controllare la tabella delle connessioni per capire che quel pacchetto non fa parte di una connessione attiva e scartarlo.

[iSt]

3.4 Svantaggi nell'uso del Firewall

Detti i pregi dei Firewall dobbiamo parlare anche degli svantaggi che questa tecnologia comporta. Di seguito possiamo elencare e riassumerne alcuni:

- Mancanza di protezione per minacce interne alla rete

  Come ben sappiamo i firewall ci proteggono da minacce esterne alla rete, ma cosa succede se la minaccia si trova all'interno della nostra rete? Ad esempio, se un collega inavvertitamente aprisse una mail con un allegato che poi si riveli essere un malware che si diffonde tramite la rete un firewall non sarebbe in grado di proteggerci, in quanto la minaccia si trova sulla nostra stessa sottorete.

  Si pone come eccezione il NextGen Firewall che ha funzionalità per proteggere la rete dai malware.

- Costi di manutenzione e gestione

  Un aspetto potenzialmente svantaggioso legato all'utilizzo di un firewall riguarda i suoi costi di manutenzione e gestione. Dovremmo assumere nel caso di un'azienda un amministratore di rete che mantenga il sistema attivo e aggiornato.

  Inoltre, c'è il costo iniziale per, ad esempio, l'acquisto di un firewall hardware, ma anche il costo di una licenza nel caso si utilizzi un firewall software non open source.

- Regole del firewall più complesse da formulare per grandi aziende

  Per una piccola azienda la configurazione di un firewall risulta relativamente semplice. Ma per un'impresa di grandi dimensioni ci dovranno essere uno o più amministratori di sistema che lavorino sul firewall e che si troveranno a dover applicare regole complesse dettate da determinate normative aziendali per garantire la sicurezza della rete. Quindi, cambiare le policy del firewall diventa un lavoro molto più complesso.

- Problemi di connettività con alcune applicazioni

  Potrebbero esserci problemi di connettività con applicazioni che utilizzano un dato protocollo che il firewall blocca. Per esempio, alcune applicazioni di video chiamate utilizzano come protocollo UDP che non garantisce la consegna dei pacchetti, in quanto è tollerabile la perdita di alcuni dati per questo utilizzo. Perciò se il nostro firewall blocca tutto il traffico UDP e l'applicazione non utilizza anche TCP, potrebbe non funzionare e incorrere in dei problemi di connettività.

  [iSt]

3.5 Principali firewall commerciali

- Cisco asa

  Cisco ASA (Adaptive Security Appliance) è un firewall proprietario di Cisco. E' di solito usato per il filtraggio dei pacchetti ma supporta molte altre funzionalità come la statefull Inspection, il nat , il dhcp e le vpn. Abbiamo quindi un firewall hardware che protegge la rete e in più un firewall software per proteggere i dispositivi connessi alla nostra rete. [Uni]

- Palo Alto Networks

  Il firewall fornito da Palo Alto Networks è ottimo per proteggere i sevizi cloud usati dalla compagnia. Infatti, viene utilizzata un tunnel VPN site-to-site per creare una rete virtuale protetta che include il cloud, proteggendo così i nostri

dati. Questa tecnologia utilizza solo la statefull inspection e quindi analizza solo le informazioni contenute nel header del pacchetto e non i dati contenuti nel payload come molti altri firewall fanno.

[Ste g]

- Avast Premium Security

  Avast Premium Security è un firewall commerciale che offre protezione contro i ransomware, il file encryption e il file shredder. Offre anche delle funzioni anti-phishing e antifrode per rendere più sicuro l'home banking. Fornisce anche la possibilità di proteggere la webcam dall'essere hackerata da terze parti.

  [Turno]

- Norton 360 Premium

  Norton 360 fornisce un firewall con funzionalità anche di antivirus e anti malware. Include anche una VPN, il parental control, password manager e backup online del cloud. C'è anche una funzionalità che avvisa se i nostri dai sono apparsi in vendita nel Dark Web.

  [Turno]

- McAfee

  McAfee offre un servizio firewall unito ad un software antivirus. Esso ha funzionalità di antispam, protezione dal furto di identità e un software per cancellare i file in modo permanente. Ogni firewall supporta fino a cinque dispositivi.

  [Ste g]

3.6 Principali firewall gratuiti

- Pfsense

  PfSense è un firewall basato su freeBSD. Esso è open source. Può essere aggiornato e manutenuto tramite la sua interfaccia web e non richiede la conoscenza della sottostante sistema freeBSD per essere gestito. Verrà descritto in modo più approfondito nel prossimo capitolo.

  [Wikg]

- Windows Defender

  Windows Defender è il firewall gratuito installato e attivo di default sulle distribuzioni Windows più recenti. È molto semplice da configurare, basta cercarlo nel menu start di Windows. Dal menù si possono modificare le impostazioni e creare nuove regole o anche eventualmente disabilitarlo.

  [Turno]

- Uncomplicated Firewall

  Uncomplicated Firewall (UFW) è un firewall a linea di comando che ha dei comandi molto semplici e usa le iptables per la configurazione. È disponibile di default in tutte le distribuzioni Ubuntu successive alla 8.04 LTS.

  Gufw è l'interfaccia grafica per rendere più semplice la configurazione e l'uso di Uncomplicated Firewall.

[Wikh]

- Comodo Firewall

  Comodo Firewall è un firewall gratuito che ha funzionalità come il controllo del traffico, il nascondere le porte del pc agli hackers e bloccare i malware dal trasmettere i dati privati all'esterno.

  Include anche un browser sicuro per navigare in internet. Ha la funzionalità di host intrusion protection system (HIPS). L'HIPS si accorgerà del comportamento malevolo di un programma e ti chiederà se bloccare o permettere la sua esecuzione.

  Include anche le sue versioni più sicure di browser come Chrome e Firefox rispettivamente con il nome di Dragon e IceDragon

  Offre anche un sandbox chiamata Comodo's Virtual Kiosk per eseguire applicazioni sconosciute in un ambiente sicuro.

  [Turno]

- TinyWall

  TinyWall è progettato per essere usato con Windows Defender quindi il suo impatto sulle prestazioni è minimo.

  Ha funzionalità come il blocco dei malware e l'impedire hai malware di modificare le impostazioni di Windows Defender. Tutto questo con senza dover avere conoscenza di porte e protocolli da bloccare.

  La caratteristica più interessante e il non usare pop up, per garantire l'accesso ad Internet o negarlo, come su altri firewall.

  TinyWall preferisce un approccio diverso utilizzando whitelist per i programmi che richiedono l'accesso a internet. L'utente aggiungerà semplicemente un nuovo programma alla whitelist è garantirà ad esso l'accesso ad Internet in un modo molto intuitivo.

  [Turno]

4. Pfsense

4.1 Cos'è Pfsense?

PfSense è un firewall open source basato su freeBSD. Non è necessaria alcuna conoscenza del sistema operativo sottostante per farlo funzionare.

Basta collegarsi alla sua interfaccia web per configurarlo o aggiornarlo.

Esso oltre alla funzionalità di firewall/routing permette di personalizzare la nostra configurazione con servizi quali il captive portal, la vpn, antivirus e tanti altri.

Oltre ad essere una potente piattaforma firewall e router, essa include una lunga lista di pacchetti che permettono di espandere facilmente le funzionalità senza compromettere la sicurezza del sistema.

Sempre tramite questa interfaccia è possibile aggiungere delle nuove funzionalità come un proxy server come Squid, l'url filtering con SquidGuard e tante altre.

4.2 Funzionalità di Pfsense

Le principali funzionalità che sono state utilizzate all'interno di questa tesi con Pfsense sono state il Captive Portal, il Proxy server E il port Forwarding.

- Captive Portal

  Il captive portal permette di forzare l'autenticazione o ridirigere il traffico di rete ad una pagina di autenticazione di rete.

  Questo è comunemente usato nelle connessioni di rete hot-spot, ma anche ampiamente usata per livelli di sicurezza aggiuntivi nell'accesso delle reti Internet attraverso i sistemi wireless.

  Nel nostro caso è servito per far autenticare i docenti e gli studenti quando si collegavano ad internet dalla loro macchina. L'autenticazione è stata effettuata mediante la funzionalità di Pfsense che permette di sfruttare l'autenticazione con Active Directory che si trova installato sul server Microsoft.

- Proxy Server

  Come proxy server si è usato il software Squid che è stato aggiunto a Pfsense mediante la sua interfaccia web. Oltre a Squid sono stati installati anche SquiGuard e LightSquid.

  Il proxy è molto semplice ed intuitivo da configurare. In questa tesi si è preferito usare un transparent proxy con la cattura anche del traffico https.

Il trasparent proxy ci da il grande vantaggio rispetto ad un proxy tradizionale di non dover configurare nulla sul browser della macchina che all'interno della rete prova a collegarsi ad internet.

Inoltre, grazie a SquidGuard è stato possibile utilizzare delle blacklist per bloccare un insieme di siti già predisposti e suddivisi per categorie.

Con LightSquid invece abbiamo accesso a tutte le statistiche raccolte dal proxy permettendoci di monitorare quali siti vengono visitati e con che frequenza e se ci si era provati a collegare a siti che erano stati bloccati.

- Port Forwarding

  Il port forwarding è una tecnica che permette di esporre un nostro servizio interno al di fuori della nostra rete locale. Nel nostro caso il server web si trova all'interno della lan e per rendere visibile il sito web della scuola all'esterno si è usata questa tecnica per inoltrare il traffico al server Windows che ospita il sito web della scuola.

  [Keafe]

4.3 Guida all'installazione di Pfsense

Per installare Pfsense basta cercare in rete il link per il download e scaricare la ISO. Poi si crea la macchina virtuale con VirtualBox e si segue il wizard per l'installazione di Pfsense. Di seguito viene fornito un link di riferimento al sito Ufficiale di Pfsense da cui è possibile scaricare la versione che si desidera.

Link iso Pfsense:

https://www.pfsense.org/download/

5. Windows Server

5.1 Cos'è windows server?

Windows Server è il nome di una distribuzione ideata da Microsoft per essere installata in un server. Essa semplifica l'uso e le gestioni delle reti di calcolatori indipendentemente dal numero di host che sono collegati e offre diverse funzioni come dns, active directory, web server, server di stampa e molte altre.

Permette inoltre di applicare dei criteri di gruppo per determinati utenti e di condividere al meglio le risorse di rete tra i vari host.

La versione che abbiamo usato in questa tesi è quella di prova con validità 180 giorni di Windows Server 2012 R2

5.2 Funzionalità di Windows Server

Le principali funzionalità che sono state utilizzate all'interno di questa tesi con Windows Server sono state le policy di gruppo, active directory per autenticarsi al captive portal e il server web per pubblicare il sito della scuola.

- Active Directory

  In Windows Server Active Directory è una tecnologia che si basa sui concetti di dominio cioè un gruppo di calcolatori che condividono un database di risorse di rete e che sono controllati con delle policy di gruppo e di directory ovvero un insieme di servizi di rete gestiti da un domain controller.

  Active Directory permette di sfruttare delle policy di gruppo per definire come le risorse di rete vengono distribuite tra gli utenti del dominio. Infatti, in Active Directory si ha un unico sistema per controllare tutti gli oggetti presenti sul server come gli utenti, i servizi come il server mail e le risorse ovvero le stampanti.

  Con Active Directory e in particolare grazie al servizio di autenticazione Kerberos si riesce ad utilizzare il Single Sign-On in modo che l'utente una volta autenticato può sfruttare tutte le risorse della rete senza dover effettuare di nuovo l'autenticazione.

  Nella terminologia di Active Directory ritorneranno in seguito dei nomi in particolare unità organizzativa, utente, computer e gruppo.

  L'unità organizzativa è un contenitore di oggetti che appartengono allo stesso dominio. Essa verrà utilizzata per contenere gli oggetti che verranno creati come i gruppi gli utenti e i computers.

  Ad essa inoltre verranno come si vedrà meglio nel seguito collegate le policy di gruppo che verranno poi applicate.

I gruppi invece sono utilizzati per collezionare gli utenti e rendere più facile l'applicazione di criteri di gruppo.

Infine, ci sono gli utenti e i computers: i primi servono ad assegnare ad ogni utente il rispettivo accesso alle risorse di rete, mentre i secondi sono semplicemente i pc che si sono uniti al dominio.

[Alllu]

[Wika][Wikc]

- Group Policy

  Con le group policy si creano degli oggetti chiamati group policy object che possono essere applicati a gruppi di utenti e hai loro rispettivi computer. Con le policy riusciamo a controllare in modo molto semplice e in maniera centralizzata i computer e gli utenti applicando regole per limitare determinate azioni ritenute dannose all'interno di un'azienda come l'auto play dei media esterni, l'utilizzo del pannello di controllo l'accesso a determinate cartelle del sistema.

  Con le policy di gruppo si possono anche condividere risorse di rete con singoli gruppi di utenti come, ad esempio, le stampanti o possiamo anche impostare uno sfondo del pc con il logo dell'azienda su tutti gli host del dominio.

  [Wikf]

- Server Web

  Il server web che abbiamo usato è stato quello fornito da Windows sul suo server. È molto semplice da installare e configurare come si vedrà in seguito nel capitolo 6.3.3. Esso ci ha permesso di ospitare il sito web della scuola.

5.3 Guida all'installazione di Windows Server

Per installare Windows Server basta cercare in rete la versione di prova gratuita con validità 180 giorni e scaricare la ISO. Poi si crea la macchina virtuale con VirtualBox e si segue il wizard per l'installazione del server. Di seguito viene fornito un link di riferimento al sito Microsoft con le versioni di prova.

Link iso Windows Server 2012:
https://www.microsoft.com/it-it/evalcenter/evaluate-windows-server-2012-r2

6. Caso di studio un rete scolastica

6.1 I principali problemi da risolvere

I principali problemi da risolvere sono: autenticare gli studenti e i docenti con captive portal tramite active directory, creare delle policy per gli studenti e i docenti, rendere disponibile tramite il server web il sito internet della scuola e filtrare il traffico con il proxy Squid.

Nell'immagine sottostante possiamo vedere come è stata progettata la rete del nostro caso di studio.

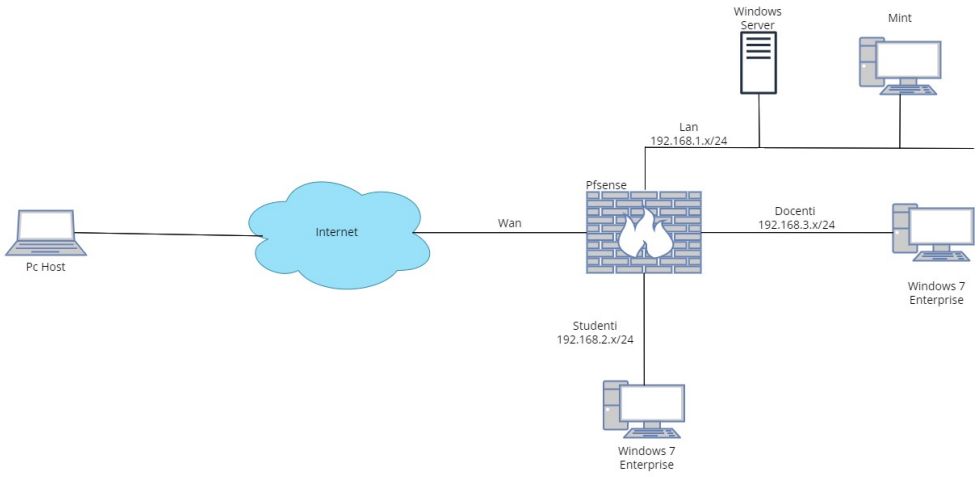


Figura 6.1: Progetto della rete del caso di studio

6.2 Configurazione Iniziale

Per prima cosa installiamo le seguenti macchine virtuali per la nostra prova. Nelle Immagini di seguito si vedono i parametri che sono stati utilizzati per la prova come quantità di ram, numero e schede di rete a cui le macchine sono collegate. Le macchine Pfsense devono avere quattro schede di rete: la prima in bridge con la scheda fisica del pc, la seconda collegata alla rete privata che sarà la nostra rete amministrativa senza restrizioni e captive portal. La terza invece sarà la rete alla quale si collegano gli studenti e la quarta invece individuerà la rete dei docenti.

La macchina mint verrà utilizzata per configurare Pfsense tramite il suo web configurator e si troverà nella sotto rete dell'amministrazione. Windows server si troverà

nelle schede di rete dell'amministrazione.

Pfsense	4 schede di rete una in bridge una in rete interna e due in soloHost	4Gb ram
Windows Server 2012 R2	1 scheda di rete collegata alla rete interna	4Gb ram
Macchina Windows 7 Studente1	1 scheda di rete collegata alla rete soloHost2	1Gb ram
Macchina Windows 7 Docente1	1 scheda di rete collegata alla rete soloHost3	1Gb ram
Macchina Mint (per configurare Pfsense)	1 scheda di rete collegata alla rete interna	4Gb ram

Tabella 6.1: Configurazione macchine virtuali

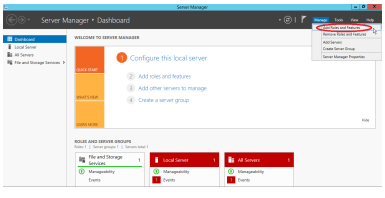
Installate tutte le macchine e collegate alle schede di rete corrette possiamo iniziare a lavorare sul server.

6.3 Installazione dei servizi su Windows Server

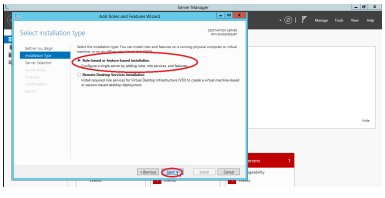
In questa sezione vedremo come installare i servizi su Windows Server che sono stati usati nello svolgimento della tesi.

6.3.1 Installare active directory

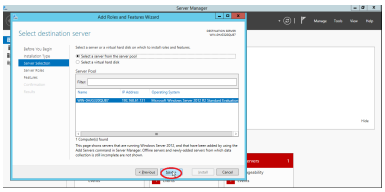
Andiamo sul server manager e andiamo su aggiungi ruoli e funzioni. Clicchiamo su avanti e scegliamo istallazione basata sui ruoli e nella prossima schermata scegliamo il server su cui effettuare l'installazione. Selezioniamo ruoli di active directory e poi aggiungiamoli al server. Andiamo avanti fino alla schermata in cui ci viene chiesto di effettuare l'installazione e clicchiamo su installa. Dalla schermata principale del server manager clicchiamo sulla flag e promuoviamo il server a domain controller. Nel wizard selezioniamo nuova foresta e diamo il nome al dominio. Seguiamo il wizard fino ad arrivare alla verifica dei requisiti e clicchiamo su installa. Il server verrà riavviato e sarà adesso un dominio di active directory.



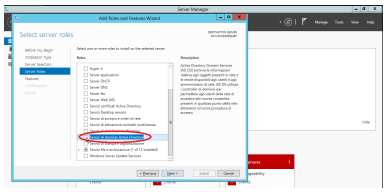
(a) Schermata del Server Manager



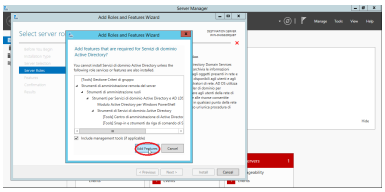
(b) Scegliamo il tipo di installazione



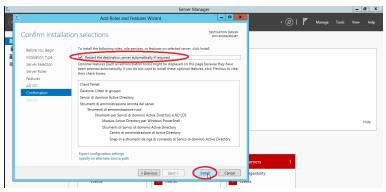
(c) Selezioniamo il server per l'installazione



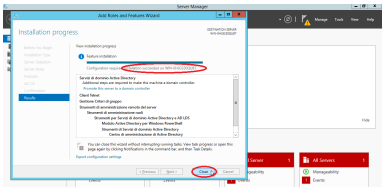
(d) Selezioniamo servizi di active directory



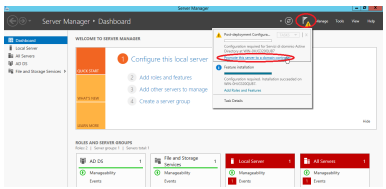
(e) Aggiungiamo la feature al server



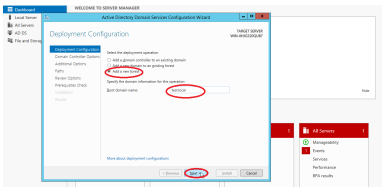
(f) Selezioniamo installa



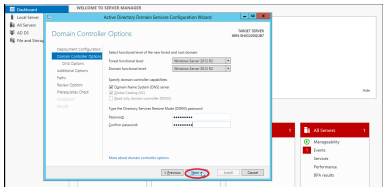
(g) Installazione conclusa con successo



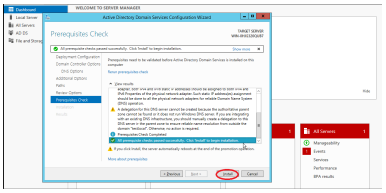
(h) Promuoviamo il server a Domain Controller



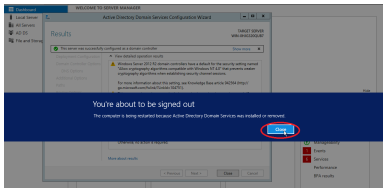
(i) Creiamo una nuova foresta e diamo un nome al dominio



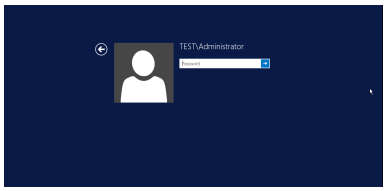
(j) mettiamo la password per il ripristino e clicchiamo next



(k) Verifica dei requisiti e inizio installazione



(l) Riavvio server per completare l'installazione

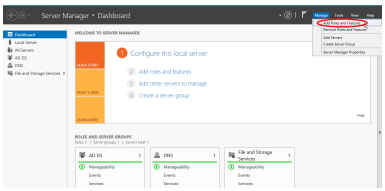


(m) I servizi di active directory
sono stati installati

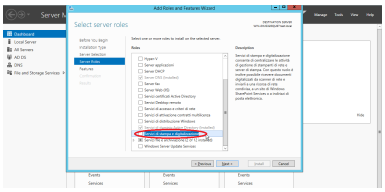
Figura 6.2: Installazione di Active Directory

6.3.2 Installare server Stampa

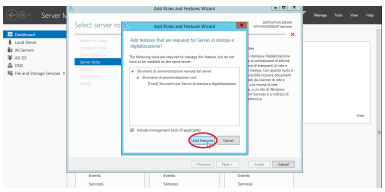
Andiamo sul server manager e andiamo su aggiungi ruoli e funzioni. Clicchiamo su avanti e scegliamo istallazione basata sui ruoli e nella prossima schermata scegliamo il server su cui effettuare l'installazione. Selezioniamo i servizi di stampa e digitalizzazione. Seguiamo il wizard per l'installazione fino alla fine e clicchiamo installa e avremo così installati il server di stampa.



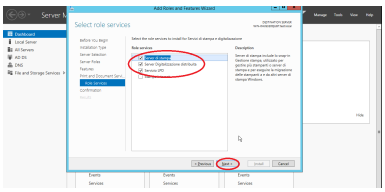
(a) Schermata del Server Manager



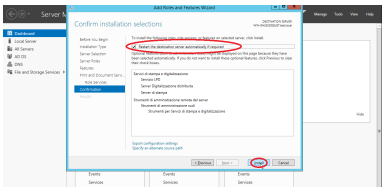
(b) Scegliamo i servizi di stampa e digitalizzazione



(c) Aggiungiamo la feature al server



(d) Personalizziamo l'installazione

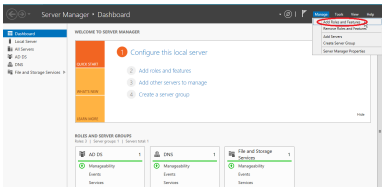


(e) Clicchiamo su installa

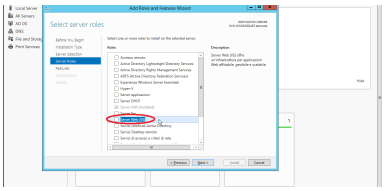
Figura 6.3: Installazione del server di stampa

6.3.3 Installare server web

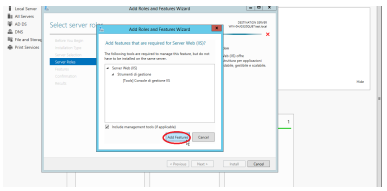
Andiamo sul server manager e andiamo su aggiungi ruoli e funzioni. Clicchiamo su avanti e scegliamo istallazione basata sui ruoli e nella prossima schermata scegliamo il server su cui effettuare l'installazione. Selezioniamo server web (IIS) . Seguiamo il wizard per l'installazione fino alla fine e clicchiamo installa e avremo così installati il server web.



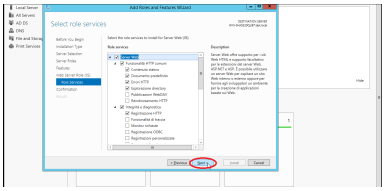
(a) Schermata del Server Manager



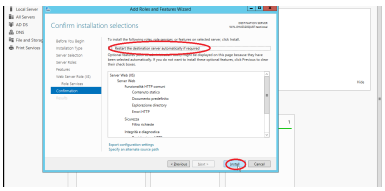
(b) Scegliamo servizi web (IIS)



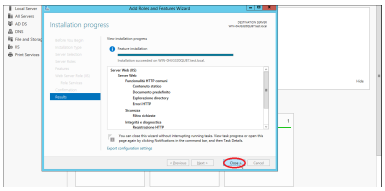
(c) Aggiungiamo la feature al server



(d) Clicchiamo next



(e) Clicchiamo su installa



(f) Installazione eseguita con successo

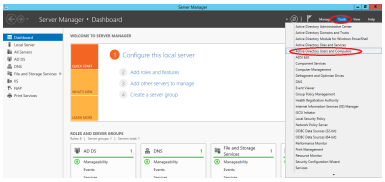
Figura 6.4: Installazione del server web

6.4 Configuriamo Windows Server

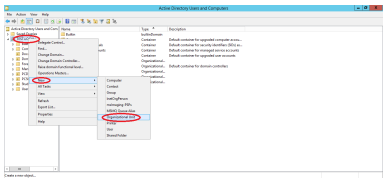
In questa sezione vedremo come configurare il windows server per i nostri scopi all'interno di una rete scolastica.

6.4.1 Creare una nuova unità organizzativa

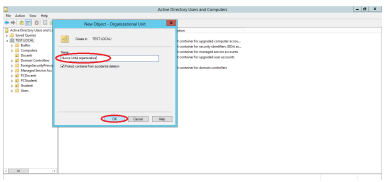
Per creare un'unità organizzativa dalla schermata del server manager selezioniamo strumenti e poi active directory utenti e computers. Clicchiamo con il tasto destro sul dominio che abbiamo creato e dal menù a tendina selezioniamo nuova e poi unità organizzativa. Compiliamo il wizard con i dati e abbiamo così creato una nuova unità organizzativa.



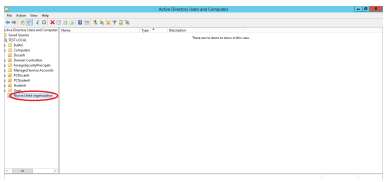
(a) Scegliamo active directory users and computers



(b) Clicchiamo sul dominio scegliamo nuova e poi unità organizzativa



(c) Inseriamo il nome e diamo ok

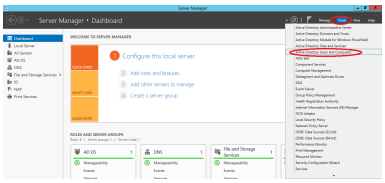


(d) La nuova unità organizzativa è stata creata

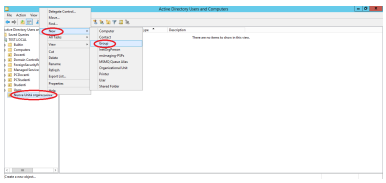
Figura 6.5: Creare una nuova unità organizzativa

6.4.2 Creare un nuovo gruppo

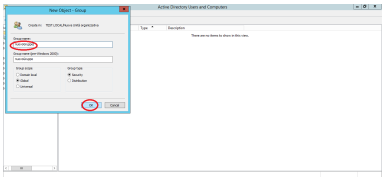
Per creare un nuovo gruppo dalla schermata del server manager selezioniamo strumenti e poi active directory utenti e computers. Clicchiamo con il tasto destro sull'unità organizzativa nella quale vogliamo creare un nuovo gruppo e dal menù a tendina selezioniamo nuova e poi gruppo. Compiliamo il wizard con i dati e abbiamo così creato un nuovo gruppo.



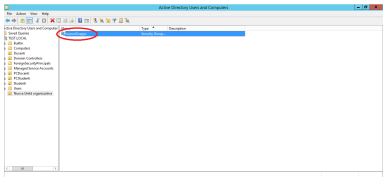
(a) Scegliamo active directory users and computers



(b) Selezioniamo un' unità organizzativa e creiamo un nuovo gruppo



(c) Inseriamo il nome del nuovo gruppo e diamo ok



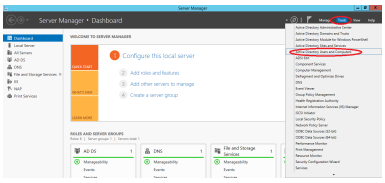
(d) Il nuovo gruppo è stato creato

Figura 6.6: Creare un nuovo gruppo

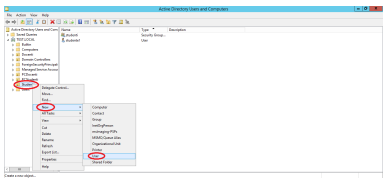
6.4.3 Aggiungere gli utenti

Per creare un nuovo utente dalla schermata del server manager selezioniamo strumenti e poi active directory utenti e computers. Clicchiamo con il tasto destro sull'unità organizzativa nella quale vogliamo creare un nuovo utente e dal menù a tendina selezioniamo nuova e poi utente. Compiliamo il wizard con i dati e abbiamo così creato un nuovo utente.

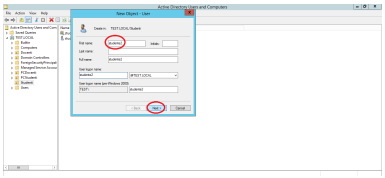
Attenzione: Ricordarsi di aggiungere l'utente al gruppo. Come spiegato nella prossima sezione.



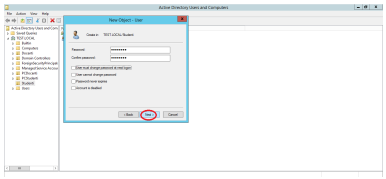
(a) Scegliamo active directory users and computers



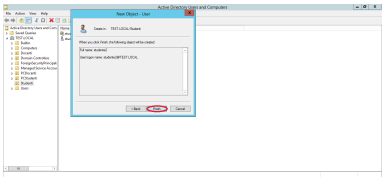
(b) Selezioniamo un'unità organizzativa e creiamo un nuovo utente



(c) Impostiamo il nome



(d) Impostiamo la password

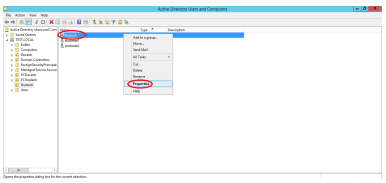


(e) Clicchiamo su fine nel riepilogo

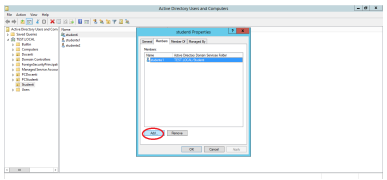
Figura 6.7: Aggiungere gli utenti

6.4.4 Aggiungere un utente ad un gruppo

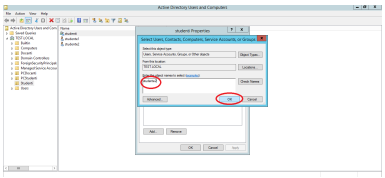
Per aggiungere un utente ad un gruppo clicchiamo con il tasto destro sopra un gruppo già creato e dal menù scegliamo le proprietà. Andiamo su membri e clicchiamo aggiungi, cerchiamo l'utente da aggiungere e clicchiamo su applica. Abbiamo così aggiunto un nuovo utente ad un gruppo.



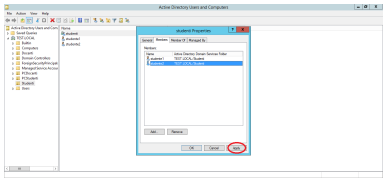
(a) Selezioniamo un gruppo e apriamo le proprietà



(b) Clicchiamo su aggiungi



(c) Cerchiamo l'utente da aggiungere mediante il nome



(d) Clicchiamo su applica per aggiungere l'utente al gruppo

Figura 6.8: Aggiungere un utente ad un gruppo

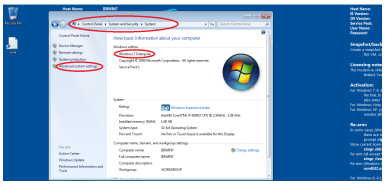
6.4.5 Aggiunta di un pc al dominio

Apriamo il pannello di controllo di Windows e andiamo su Sistema e sicurezza e poi sistema. Controlliamo che la versione di windows sia pro o superiore. Clicchiamo su impostazioni di sistema avanzate. Clicchiamo su rinomina il computer o cambia il suo domino o workgroup. Selezioniamo il nome che vogliamo dare al pc e il domino nel

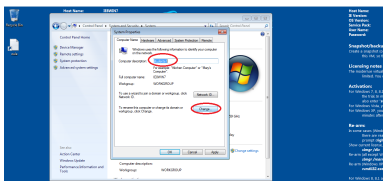
mio caso studente1 e scuola.local. Va precisato che avremo un errore se non abbiamo già aggiunto il record dns per il server sul quale abbiamo installato active directory. Per farlo basta andare su Pfsense e poi Dns resolver e aggiungere un nuovo record. Se il record esiste una volta impostati il nome e il dominio cliccando su ok si aprirà una finestra dove dovremo inserire le credenziali di active directory. Seguiamo il wizard e una volta completato il pc sarà riavviato e potremo vedere che è stato unito al dominio.

Nota Bene: Per aggiungere un pc ad un dominio occorre windows versione pro o superiore.

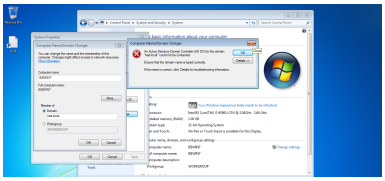
Attenzione: Ricordarsi di aggiungere il record per il Server di active directory sul Dns resolver di Pfsense.



(a) Pannello di controllo Pc da aggiungere

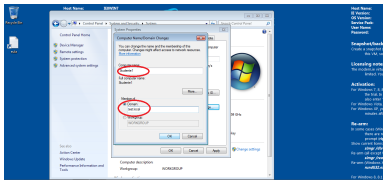


(b) Pannello di controllo Pc da aggiungere

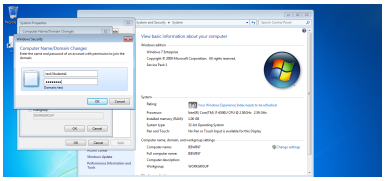


(c) Errore DNS

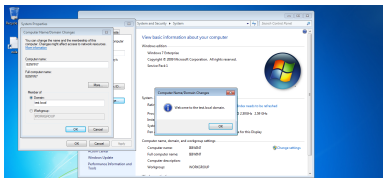
(d) Pfsense aggiunta Dns



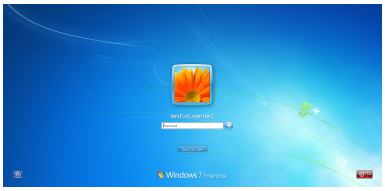
(e) Pannello di controllo Pc da aggiungere



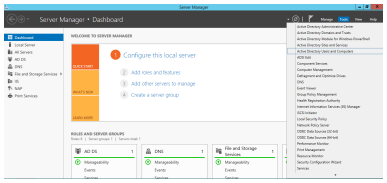
(f) Pannello di controllo Pc da aggiungere



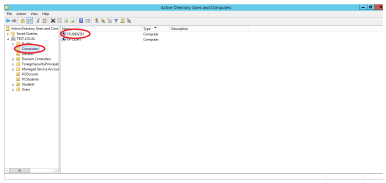
(g) Pannello di controllo Pc da aggiungere



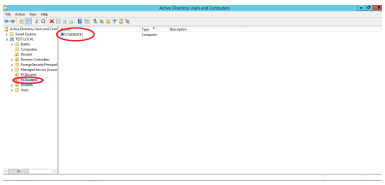
(h) Schermata avvio Pc



(i) Windows Server Active Directory Users and Computers



(j) Windows Server Computers



(k) Windows Server Pc Studenti

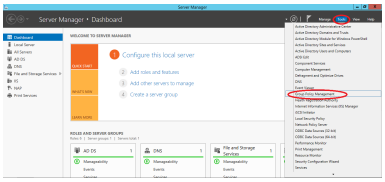
Figura 6.9: Aggiunta di un pc al dominio

6.4.6 Group policy per studenti e docenti

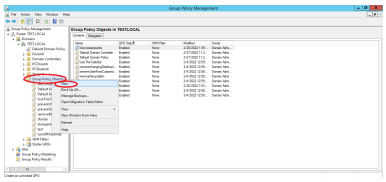
In questa sezione verrà illustrato come applicare una policy ad un gruppo specifico. La procedura descritta è la medesima sia per i docenti che per gli studenti. In questo caso vedremo un esempio di applicazione di una policy al gruppo degli studenti per bloccare l'accesso al pannello di controllo.

Dal server manager clicchiamo su strumenti e poi su gestore criteri di gruppo. Dal menu a sinistra clicchiamo su oggetti policy di gruppo e clicchiamo su nuova. Diamogli un nome significativo alla policy nel nostro caso BloccoPannelloControllo. Una volta creata la policy clicchiamo su di essa con il tasto destro e scegliamo edita. Da qui scegliamo il percorso Configurazioni utente/policy/Impostazioni di Windows/template amministrativi/ pannello di controllo. Qui dalla finestra a destra selezioniamo Proibire l'accesso al pannello di controllo e le impostazioni del pc. Si aprirà una finestra dove cliccheremo abilita e applica. La policy e così creata. Adesso delle Unità organizzativa degli studenti e dobbiamo cliccare con il tasto destro e selezionare Link an existing GPO e scegliamo la policy appena creata. La stessa cosa va fatta per l'unità organizzativa dei PC Studenti. Adesso clicchiamo sulla policy e nel campo secure filtering aggiungiamo il gruppo degli studenti. abbiamo così creato una policy di gruppo funzionante.

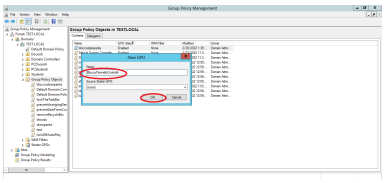
Nota Bene: Molte policy vengo applicate al riavvio del pc, e per questo se il pc e già acceso non verranno applicate. Si può forzare per alcune policy l'aggiornamento digitando nel prompt dei comandi di Windows il comando **gpupdate /force** . Ma per altre è proprio necessario il riavvio del computer.



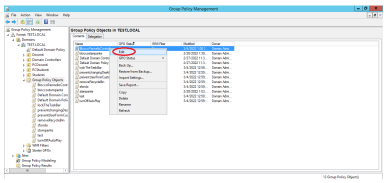
(a) Scegliamo group policy management



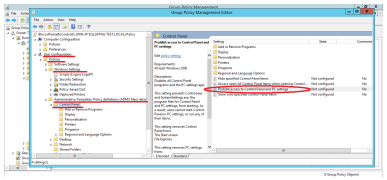
(b) Creiamo una nuova Group policy



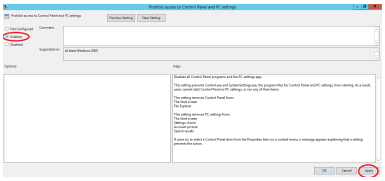
(c) Inseriamo un nome per la policy



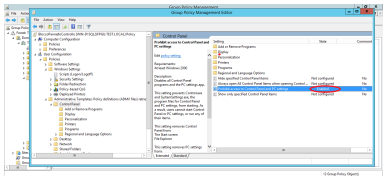
(d) Editiamo la policy



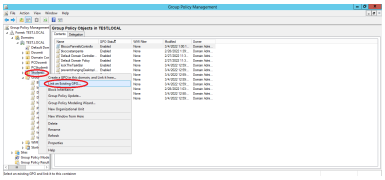
(e) Scegliamo l'opzione per bloccare il pannello di controllo



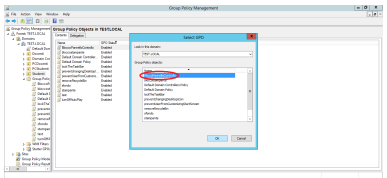
(f) Attiviamo e applichiamo la policy



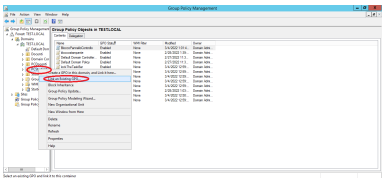
(g) Controlliamo che la policy sia abilitata



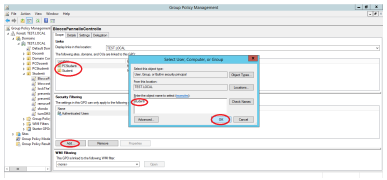
(h) Linkiamo la policy agli studenti



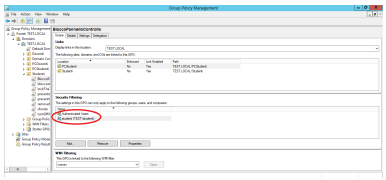
(i) Scegliamo la policy appena creata



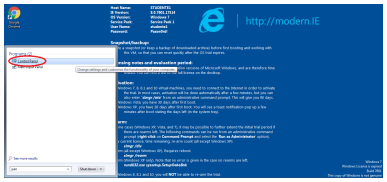
(j) Linkiamo la policy al PC Studenti



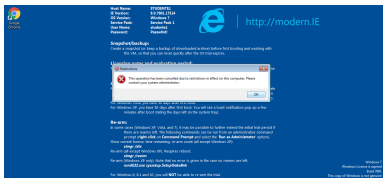
(k) Aggiungiamo il gruppo degli studenti su security filtering



(l) Controlliamo che sia stato aggiunto il gruppo studenti



(m) Cerchiamo il pannello di controllo su PC Studenti

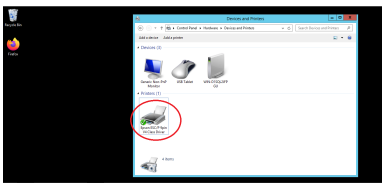


(n) Il pannello è stato bloccato correttamente

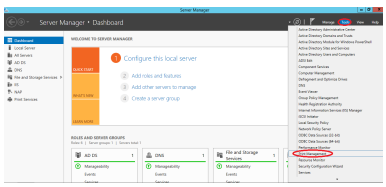
Figura 6.10: Group policy per studenti e docenti

6.4.7 Distribuzione di una stampante tramite policy di gruppo

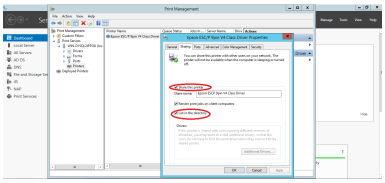
Andiamo sul server e dal pannello di controllo selezioniamo hardware e poi su devices and printers e installiamo la nostra stampante. Torniamo sulla scherma del server manager e andiamo su tools e poi selezioniamo print management. Selezioniamo la stampante che desideriamo e andiamo sulle sue proprietà. Andiamo su sharing e spuntiamo Share this printer e List in the directory e diamo ok. Selezioniamo di nuovo la stampante e dal menù a tendina scegliamo deploy with group Policy. Selezioniamo la policy che vogliamo usare se non l'abbiamo creata va prima creata. Spuntiamo the users that this gpo applies e the computer that this gpo applies e clicchiamo su applica. Avremo un messaggio di conferma che tutto è andato correttamente. Possiamo verificare che la stampante e stata distribuita cliccando su deployed printers. Dal pc sul quale vogliamo installare la stampante andiamo nel pannello di controllo e installiamo la stampante scegliendola da quelle di rete. E seguiamo la procedura per installarla.



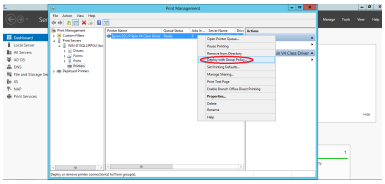
(a) Installiamo la stampante sul server



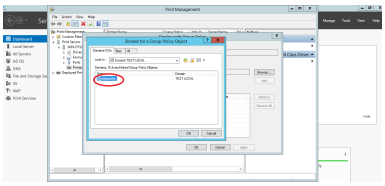
(b) Andiamo su print management



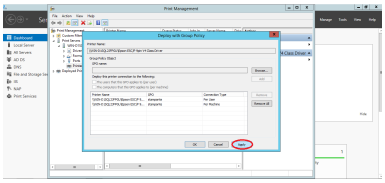
(c) Selezioniamo le impostazioni della stampante



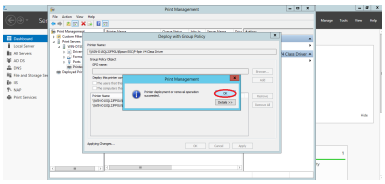
(d) Scegliamo Distribuisci con policy di gruppo



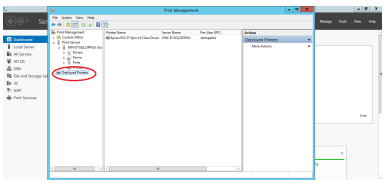
(e) Scegliamo la policy



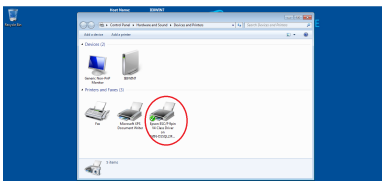
(f) Mettiamo la spunta su utenti e pc a cui si applica la policy



(g) La stampante è stata distribuita con successo



(h) Controllo che la stampante si trovi nella lista di quelle distribuite

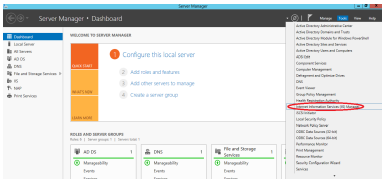


(i) Installo la stampante sui docenti

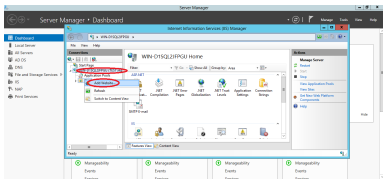
Figura 6.11: Distribuzione di una stampante tramite policy di gruppo

6.4.8 Aggiungere un nuovo sito web

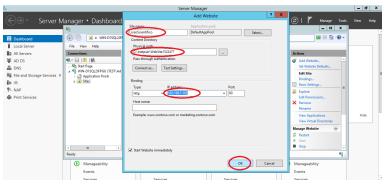
Aggiungere un nuovo sito web è molto facile, basta andare su tools e poi su ISS manager. Facciamo click sul nome del server con il tasto destro e facciamo add website. Compiliamo i campi del sito e diamo ricordandoci di inserire l'ip del server Windows. Infine, apriamo un browser all'interno della lan e proviamo a collegarci al nuovo sito appena aggiunto.



(a) Andiamo su Internet information services



(b) Aggiungiamo un nuovo sito



(c) Compiliamo i dati relativi al sito

(d) Controlliamo che il sito funzioni

Figura 6.12: Aggiungere un nuovo sito web

6.5 Configuriamo Pfsense

In questa sezione vedremo come configurare il firewall PfSense. Per prima cosa aggiungeremo le nuove reti per gli studenti e i docenti. Successivamente affronteremo l'argomento del Captive Portal e vedremo come abilitarlo ed effettuare l'autenticazione tramite Active Directory.

Vedremo anche come configurare il transparent proxy per intercettare il traffico Http e Https e abiliteremo questa tecnologia sulle reti sia degli studenti che dei docenti.

Infine, abiliteremo il Port Forwarding per esporre il nostro servizio web che ospita il sito della scuola al di fuori della lan.

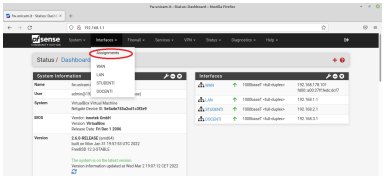
6.5.1 Configurazione della reti Studenti e Docenti

configurazione schede di rete con ip e dhcp e regole traffico

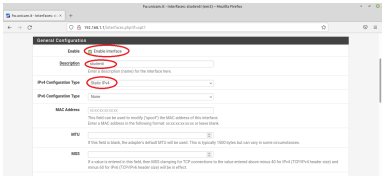
Per prima cosa andiamo sulle interfacce di PfSense e vedremo due nuove interfacce chiamate opt1 e opt2. Andiamo su opt1 e rinominiamola studenti con indirizzo ip nel range 192.168.2.1/24. Mentre su opt2 daremo il nome di docenti con ip 192.168.3.1/24

Successivamente dal menù dei servizi di PfSense abilitiamo il dhcp server su studenti con range compreso tra 192.168.2.100 e 192.168.2.200. Eseguiamo la medesima operazione sulla rete docenti ma ricordiamoci di inserire come range per il dhcp server gli indirizzi 192.168.3.100 e 192.168.3.200.

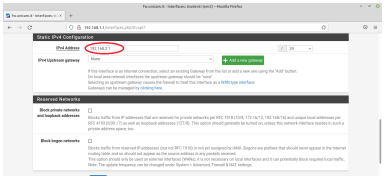
Per concludere dalle regole del firewall abilitiamo il traffico ipv4 sulle interfacce studenti e docenti.



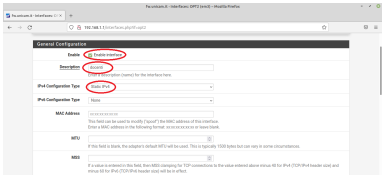
(a) Andiamo sulle interfacce



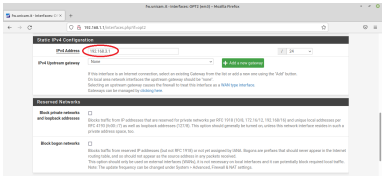
(b) Abilito l'interfaccia e la chiamo studenti A



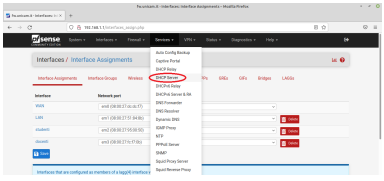
(c) Inserisco l"indirizzo ip



(d) Abilito l'interfaccia e la chiamo docenti



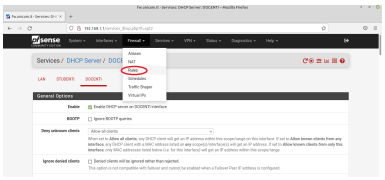
(e) Inserisco l"indirizzo ip



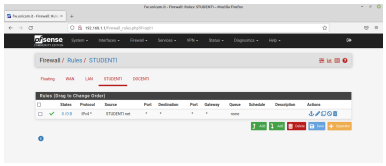
(f) Andiamo sul dhcp server

(g) Abilito il dhcp per gli studenti

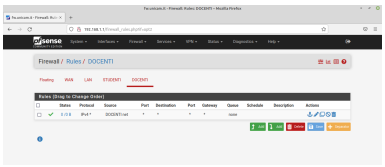
(h) Abilito il dhcp per i docenti



(i) Andiamo sulle regole del firewall



(j) Aggiungo una regola per consentire il traffico ipv4 su studenti



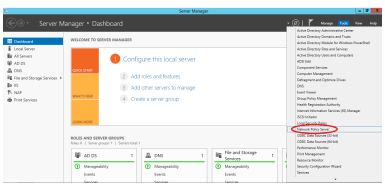
(k) Aggiungo una regola per consentire il traffico ipv4 su docenti

Figura 6.13: Configurazione della reti Studenti e Docenti

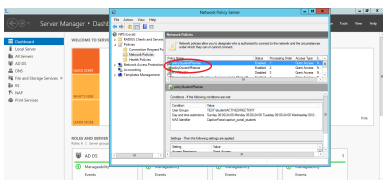
6.5.2 Configurazione del captive portal con autenticazione tramite active directory

Per prima cosa andiamo sul server e dal server manager scegliamo tools e poi Network Policy Server. Creiamo quindi due nuove policy una per gli studenti e una per i docenti. Queste policy garantiranno l'accesso sia agli studenti che hai docenti quando si collegheranno al Captive Portal. Per evitare che gli studenti possano collegarsi al Captive Portal dei docenti e viceversa nella policy impostiamo il parametro nas identifier con il valore che ci verrà fornito da Pfsense quando si collega al server. Possiamo notare che è possibile personalizzare la policy anche con gli orari in cui l'utente può connettersi.

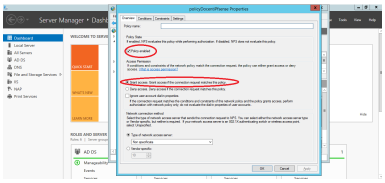
Da Pfsense invece andiamo su User Manager e poi Autentication Server e aggiungiamo il Windows Server con cui faremo l'autenticazione. Dai servizi poi di Pfsense andiamo su Captive Portal e creiamo due nuovi portali per l'autenticazione uno per i docenti e uno per gli studenti. Ricordiamoci di scegliere il Server Windows per l'autenticazione e di controllare il valore del nas identifier.



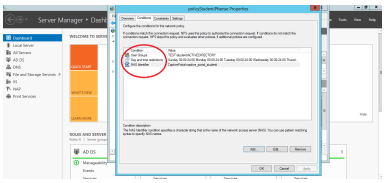
(a) Andiamo su Network Policy Server



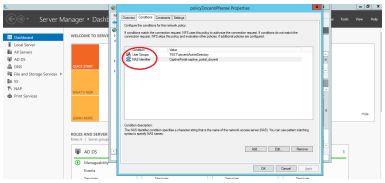
(b) Creiamo una policy per gli studenti e una docenti



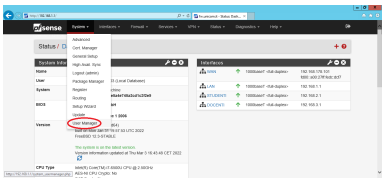
(c) Spuntiamo Grant Access



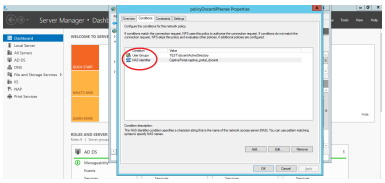
(d) Condizioni policy studenti



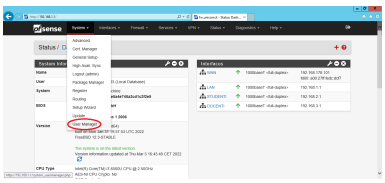
(e) Condizioni policy docenti



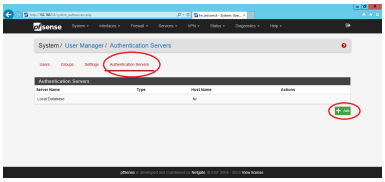
(f) Andiamo su User Manager



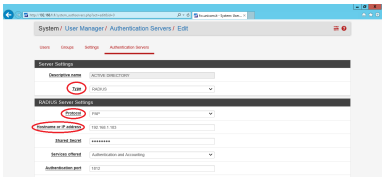
(g) Condizioni policy docenti



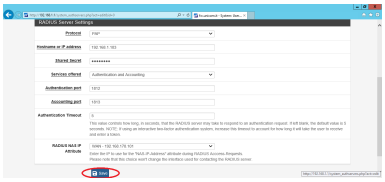
(h) Andiamo su User Manager



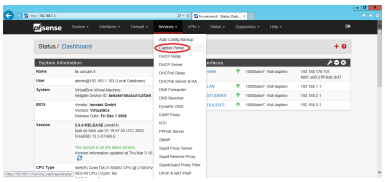
(i) Aggiungiamo un nuovo server per l'autenticazione



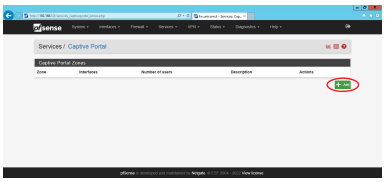
(j) Compiliamo i campi con i dati del server windows



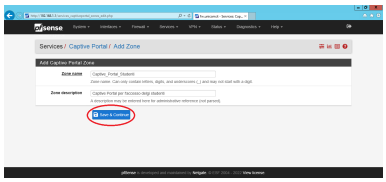
(k) Compiliamo i campi con i dati del server windows e salviamo



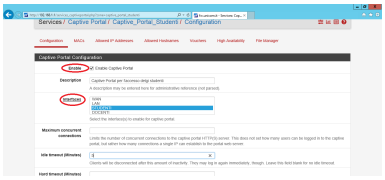
(l) Andiamo su Captive Portal



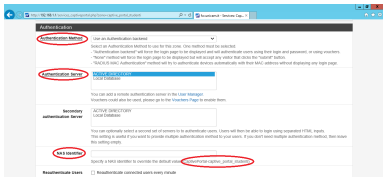
(m) Aggiungiamo un nuovo captive portal



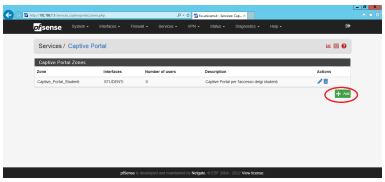
(n) Diamo un nome al captive portal



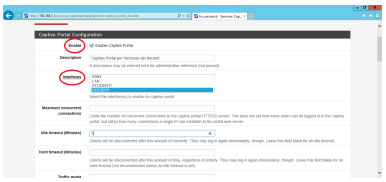
(o) Abilitiamo il captive portal e selezioniamo la rete



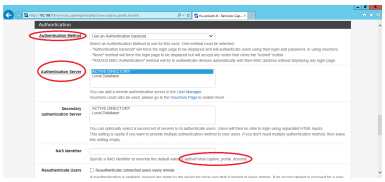
(p) Scegliamo come metodo di autenticazione Active Directory e segniamoci il Nas Identifier



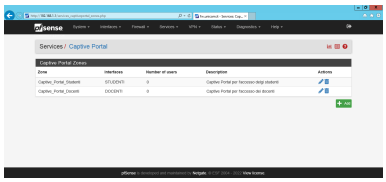
(q) Aggiungiamo un captive portal per i docenti



(r) Abilitiamo il captive portal e selezioniamo la rete



(s) Scegliamo come metodo di autenticazione Active Directory e segniamoci il Nas Identifier



(t) Abbiamo creato i captive portals

Figura 6.14: Configurazione del captive portal con autenticazione tramite active directory

6.5.3 Configurazione del transparent proxy

Andiamo sul Packet Manager e installiamo i seguenti pacchetti: Squid, SquidGuard e LightSquid.

Andiamo su Sistema, Certificate Manager e creiamo una nuova certificata autority.

Dai Servizi di Pfsense andiamo su SquidProxy Server e abilitiamo sulle interfacce degli studenti e dei docenti il proxy il transparent proxy e l'SSL filtering. Nel campo del SSL filtering aggiungiamo il CA creato precedentemente. Abilitiamo anche tutti i log. Sempre dai Servizi andiamo su SquidGuard e abilitiamolo. Abilitiamo le blacklist.

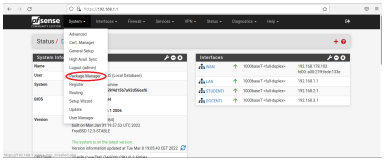
Abbiamo utilizzato la blacklist dell'Università di Toulouse perché Shallalist attualmente non è disponibile per l'attuale situazione politica mondiale.

dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

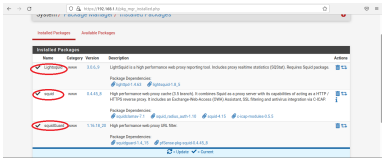
Inseriamo questo link e scarichiamo la blacklist, avremo così a disposizione diverse categorie per filtrare con delle regole il traffico internet.

Nelle immagini che seguono si può vedere una prova delle blacklist. Proviamo per prima cosa a collegarci a Facebook riuscendoci. Allora abilitiamo la regola che blocca i social network per vedere che effettivamente il sito viene bloccato. Ora mentre sulle connessioni Http Pfsense mostrerà una pagina di errore, sulle connessioni Https verrà restituito il generico errore: SSL_ERROR_RX_RECORD_TOO_LONG

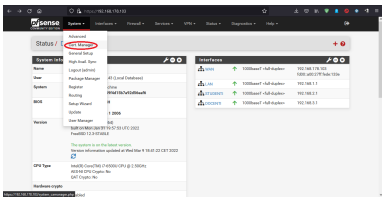
Per ulteriori approfondimenti si può consultare questo sito:https://openschoolsolutions.org/pfsense-web-filter-filter-https-squidguard/



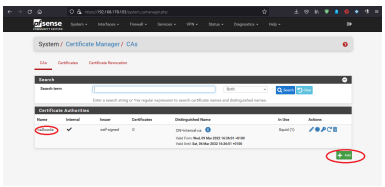
(a) Andiamo sul Package Manager



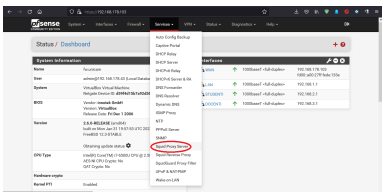
(b) Scarichiamo i pacchetti per Squid



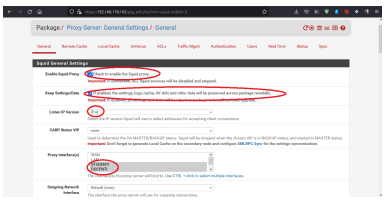
(c) Andiamo su Certificate Manager



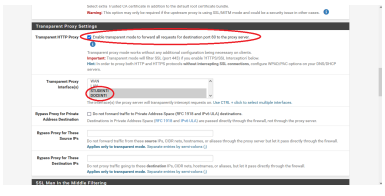
(d) Creiamo un nuovo certificato



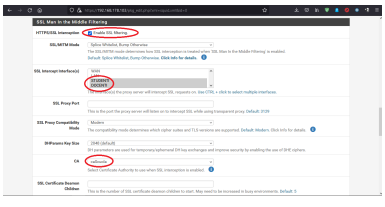
(e) Andiamo su Squid Proxy Server



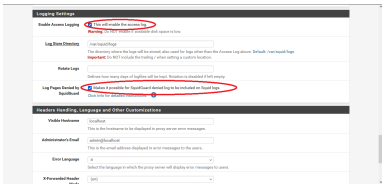
(f) Scegliamo le reti docenti e studenti



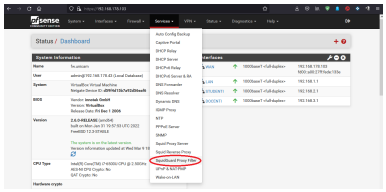
(g) Abilitiamo il Transparent Proxy



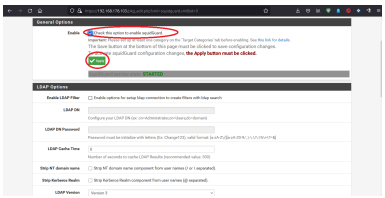
(h) Abilitiamo l' SSL Filtering



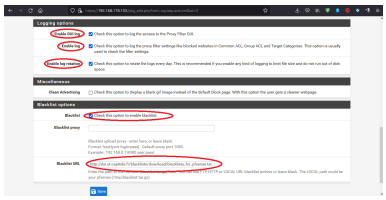
(i) Abilitiamo il log



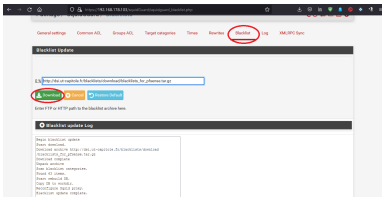
(j) Andiamo su SquidGuard Proxy Filter



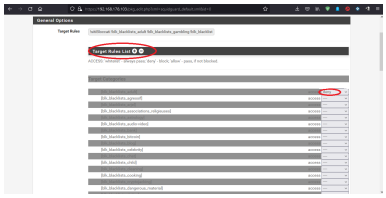
(k) Abilitiamo SquidGuard



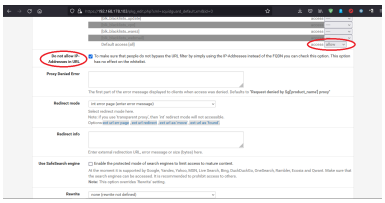
(l) Abilitiamo il log e le blacklist



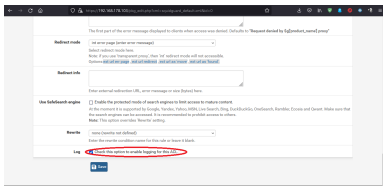
(m) Scarichiamo la blacklist



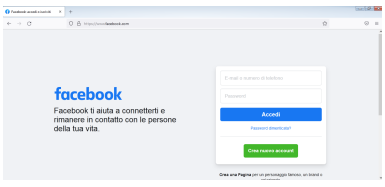
(n) Scegliamo quali filtri applicare



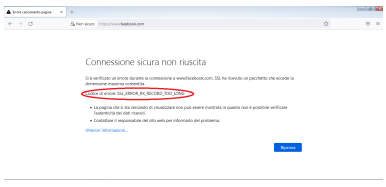
(o) Blocchiamo la ricerca dei siti tramite IP



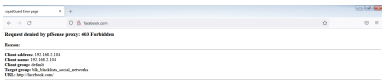
(p) Abilitiamo il log



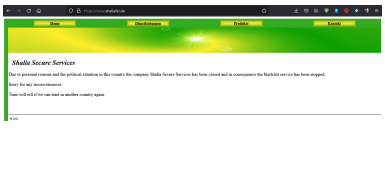
(q) Facebook funzionante prima del filtro



(r) Applico filtro Social Network errore giusto perché blocca Facebook



(s) Blocco Facebook anche in HTTP

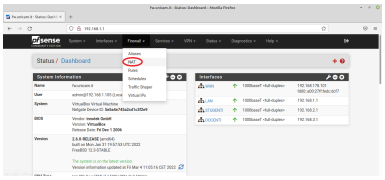


(t) ShallaList non disponibile per motivi politici

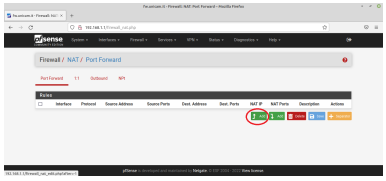
Figura 6.15: Configurazione del transparent proxy

6.5.4 Configurare il port forwarding per il server web

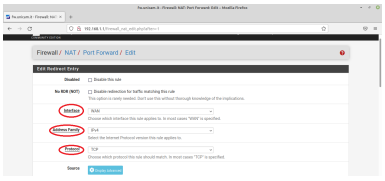
Per rendere disponibile il server web che si trova su Windows Server al di fuori della lan dobbiamo abilitare il port forwarding. Dalla schermata di Pfsense andiamo su Nat e aggiungiamo una nuova voce. Scegliamo come interfaccia in ingresso la wan e come indirizzo ip per il reindirizzamento mettiamo quello del Server Windows. Scegliamo come redirect target port quella del traffico http (80). Possiamo adesso provare a collegarci dal pc host delle macchine virtuali al ip della Wan di Pfsense e vedere che il sito della scuola sarà adesso disponibile.



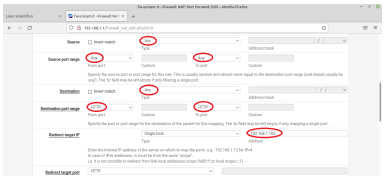
(a) Andiamo sul NAT



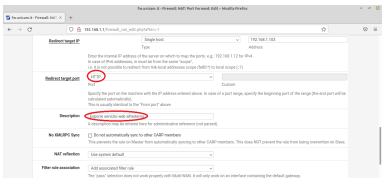
(b) Aggiungiamo una voce



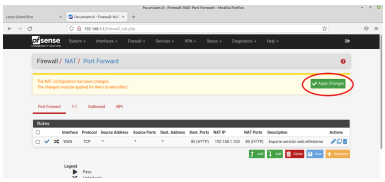
(c) Scegliamo la Wan



(d) Inseriamo l'ip del server Windows



(e) Scegliamo il traffico HTTP



(f) Controlliamo che sia stata aggiunta la voce

(g) Proviamo a collegarci dal pc host alla Wan di Pfsense: funziona!

Figura 6.16: Configurare il port forwarding per il server web

7. Conclusioni e Sviluppi Futuri

In questa tesi si è studiato il ruolo di un sistemista informatico che si trova a dover configurare una rete scolastica. Molte delle tecniche viste precedentemente sono applicabili ad altri ambienti sia domestici che aziendali.

Ad esempio, l'uso di un proxy che può essere utile a monitorare l'attività online dei figli o dei dipendenti, bloccando siti non pertinenti o dannosi.

Un eventuale sviluppo futuro per questa tesi potrebbe essere quello di migrare questo sistema in GNS3.

GNS3 è un software gratuito che permette di simulare una rete in modo reale.

I suoi utilizzi spaziano da effettuare dei semplici test, eseguire un troubleshooting dei problemi fino a gestire reti molto complesse.

Il suo funzionamento è molto semplice grazie all'interfaccia grafica che permette di realizzare delle configurazioni in modo molto veloce. È possibile utilizzare dei templete già forniti da GNS3 per aumentarne le funzioni o creare anche i nostri.

GNS3 è versatile in quanto non richiede di avere l'hardware fisico ma permette di simularlo, riducendo di sicuro i costi e rendendo più flessibile le modifiche alle configurazioni.

Sono molti i router supportati tra cui quelli Cisco.

GNS3 è utilizzato da varie agenzie, tra cui la Nasa, Google, Intel e molte altre.

[Wike][GNS]

https://www.gns3.com/software

Bibliografia

[Alllu] Robert Allen. *Active Directory Glossary – Terms and Fundamental Concepts*. 6 luglio 2019. URL: https://activedirectorypro.com/glossary/.

[And14] Jason Andress. *Network security from The Basics of Information Security (Second Edition)*. 2014. URL: https://www.sciencedirect.com/topics/computer-science/deep-packet-inspection-firewall.

[AS] Vito Carlo Speroni e Alessandro Speroni. *FIREWALL*. URL: http://www.cvsperoni.it/index.php/firewall/.

[Cis] Cisco. *Cos'è un firewall?* URL: https://www.cisco.com/c/it_it/products/security/firewalls/what-is-a-firewall.html.

[GNS] GNS3. *GNS3*. URL: https://gns3.com/.

[ion06] ionos. *Un'introduzione al concetto di virtualizzazione*. 21.06.19. URL: https://www.ionos.it/digitalguide/server/configurazione/virtualizzazione/?utm_source=pocket_mylist.

[iSt] iStarTips. *Vantaggi e svantaggi del firewall Tutto quello che c'è da sapere*. URL: https://it.istartips.com/advantages-of-firewall.html.

[IT g] intellectit Information Tecnology. *The Pros and Cons of Next Generation Firewalls*. 31 gennaio 2022. URL: https://www.intellectit.com.au/news/the-pros-and-cons-of-next-generation-firewalls/.

[Junno] JuniperNetworks. *Firewall DoS Attacks*. 8 novembre 2021. URL: https://www.juniper.net/documentation/us/en/software/junos/denial-of-service/topics/topic-map/security-routers-firewall-dos-attack.html.

[Keafe] Sam Kear. *Port Forwarding in pfSense: How to Configure NAT*. 2 febbraio 2021. URL: https://turbofuture.com/computers/Port-Forwarding-in-pfSense-How-to-Configure-NAT.

[RK17] Keith W. Ross e James F. Kurose. *Reti di calcolatori e internet. Un approccio top-down*. Milano-Torino: Pearson, 2017.

[Ste g] Courtenay Stevens. *Best Firewalls for Small Businesses 2022 Review*. 17 gennaio 2022. URL: https://www.business.org/it/cyber-security/best-firewall-for-small-business/.

[Turno] Brian Turner. *Best firewall of 2022: top paid and free services*. 9 novembre 2021. URL: https://www.business.org/it/cyber-security/best-firewall-for-small-business/#McAfee.

[Uni] Geek University. *Cisco ASA overview*. URL: https://geek-university.com/cisco-asa-overview.

[Wika] Wikipedia. *Active Directory*. URL: https://it.wikipedia.org/wiki/Active_Directory.

[Wikb] Wikipedia. *Deep packet inspection*. URL: https://en.wikipedia.org/wiki/Deep_packet_inspection.

[Wikc] Wikipedia. *Dominio*. URL: https://it.wikipedia.org/wiki/Dominio_(informatica).

[Wikd] Wikipedia. *Firewall*. URL: https://it.wikipedia.org/wiki/Firewall.

[Wike] Wikipedia. *GNS3*. URL: https://it.wikipedia.org/wiki/GNS3.

[Wikf] Wikipedia. *Group Policy*. URL: https://it.wikipedia.org/wiki/Group_Policy.

[Wikg] Wikipedia. *Pfsense*. URL: https://en.wikipedia.org/wiki/PfSense.

[Wikh] Wikipedia. *Uncomplicated Firewall*. URL: https://en.wikipedia.org/wiki/Uncomplicated_Firewall.

[Wiki] Wikipedia. *Virtualizzazione*. URL: https://it.wikipedia.org/wiki/Virtualizzazione.

Elenco delle figure

Elenco delle tabelle

A. Ringraziamenti

Ringrazio l'Università di Camerino per avermi dato la possibilità di realizzare questo traguardo della mia vita e per le opportunità che ci ha fornito.

Ringrazio il Professor Marcantoni Fausto che mi ha seguito durante questo percorso conclusivo del mio percorso formativo aiutandomi e consigliandomi al meglio.

Ringrazio la mia famiglia che mi ha sostenuto economicamente e moralmente nel corso di questi tre anni, e che mi ha spinto a dare il meglio di me.

Ringrazio la mia fidanzata Giada che mi è stata accanto in questa fase finale della mia carriera universitaria.

Ringrazio i ragazzi con cui ho abitato soprattutto Francesco che mi ha supportato (e sopportato).

Ringrazio senza un ordine particolare Pippo, Davide, Geremia e Veronica.

Ringrazio tutte le persone che mi sono state accanto e che ho incontrato in questi tre anni all'Università.

Voglio dedicare questa tesi di laurea a mio nonno scomparso due anni fa. Lui per me è stato un maestro di vita, che mi ha visto crescere e diventare un giovane adulto aiutandomi ad arrivare dove sono arrivato oggi. Sono sicuro ti sarebbe piaciuto sapere che alla fine ce l'ho fatta.

Lorenzo Santagata 13/04/2022