



# PROGETTO THETA S.P.A

UN PROGETTO DI SECURITY GRIFFINS S.P.A



# CHI SIAMO

Siamo un'azienda innovativa e versatile che opera nel settore IT con un focus speciale sulla sicurezza informatica. Offriamo consulenza IT altamente specializzata, aiutando aziende di ogni dimensione a ottimizzare i propri sistemi e a garantire la protezione delle loro risorse digitali.

La nostra missione è supportare le aziende nel loro percorso di trasformazione digitale, garantendo infrastrutture solide e sicure che permettano di concentrarsi sul core business.

## COSA FACCIAMO

- Progettazione e implementazione di infrastrutture IT
- Sicurezza informatica
- Monitoraggio e gestione della rete
- Consulenza strategica
- Testing e valutazione



# IL NOSTRO TEAM

**GRETA  
LLESHI**

**SIMONE  
BARBIERI**

**OCTAVIAN  
CERESAU**

**FRANCESCO  
FRACELLA**

**CRISTIAN  
GIRGENTI**

**LIVIU  
MIRZAC**

**FRANCESCO  
MOCCIA**

**LEONARDO  
NIGRO**

**YULIYA  
SUVOROVA**

# LA PROGETTAZIONE DI RETE

La rete è stata progettata tenendo conto della sicurezza, dell'efficienza e della gestione del traffico dati in un ambiente aziendale.

L'infrastruttura di rete utilizza vari dispositivi:

- Switch per ogni piano
- Router centrale
- Firewall perimetrale
- NAS (Network Attached Storage)
- IDS/IPS (Intrusion Detection/Prevention System).
- Web Server e Server SMTP nella DMZ

La progettazione tiene conto delle specifiche esigenze operative dei vari piani dell'edificio, che sono suddivise nelle seguenti aree funzionali:

- Piano 1/A: Front office
- Piano 1/B: Server room
- Piano 2: Ufficio vendite / Vendite online
- Piano 3: Ufficio acquisti / Consegne
- Piano 4: Amministrazione
- Piano 5: Dirigenza
- Piano 6: Reparto IT



# LA SEGMENTAZIONE DELLA RETE IN VLAN



La segmentazione della rete in VLAN è stata scelta per diverse ragioni:

- Sicurezza: Ogni piano è isolato tramite VLAN, impedendo che il traffico di rete da un piano possa essere facilmente intercettato o compromesso da altri piani. Ciò limita l'esposizione dei dati aziendali e rende più difficile per un attaccante spostarsi lateralmente nella rete.
- Efficienza: La segmentazione in VLAN riduce il dominio di broadcast, migliorando le prestazioni della rete, grazie alla riduzione del traffico di rete non necessario.
- Controllo del traffico: La divisione in VLAN permette, tramite l'implementazione di ACL, di configurare regole di accesso granulari per consentire o negare specifiche comunicazioni tra le sottoreti. Questo garantisce che solo i flussi di traffico autorizzati possano attraversare i confini tra i vari piani.

La rete è stata segmentata in 6 sottoreti distinte, ognuna corrispondente a un piano dell'edificio e associata a una VLAN. Le sottoreti e le rispettive VLAN sono le seguenti:

- VLAN 10 - Piano 1: Sottorete 192.168.10.0/24
  - VLAN 20 - Piano 2: Sottorete 192.168.20.0/24
  - VLAN 30 - Piano 3: Sottorete 192.168.30.0/24
  - VLAN 40 - Piano 4: Sottorete 192.168.40.0/24
  - VLAN 50 - Piano 5: Sottorete 192.168.50.0/24
  - VLAN 60 - Piano 6: Sottorete 192.168.60.0/24
- 

# CONFIGURAZIONE DEL ROUTER E ACCESS LISTS

Il router centrale gioca un ruolo cruciale nella gestione del traffico tra le diverse VLAN. Le ACL sono state configurate per controllare quali VLAN possano comunicare tra loro, permettendo una gestione capillare del traffico di entrata e di uscita.

## • VLAN 10

- In entrata: dalla VLAN 60
- In uscita: verso le VLAN 20,30,40

Questa configurazione permette al piano 1 front office di ricevere comunicazioni esclusivamente dal piano 6 (reparto IT) e di inviare informazioni ai piani 2 (ufficio vendite), 3 (ufficio acquisti) e 4 (amministrazione).

## • VLAN 20

- In entrata: dalle VLAN 10, 30, 60
- In uscita: verso la VLAN 10, 30

Questa configurazione permette al piano 2 (ufficio vendite / vendite online) di ricevere comunicazioni dai piani 1 (front office), 3 (ufficio acquisti), 6 (reparto IT) e di inviare informazioni ai piani 1 e 3.

## • VLAN 30

- In entrata: da VLAN 10, 20, 40, 60
- In uscita: verso le VLAN 20,40,60

Questa configurazione permette al piano 3 (ufficio acquisti) di ricevere comunicazioni dai piani 1 (front office), 2 (ufficio vendite), 4 (amministrazione) e 6 (reparto IT) e di inviare informazioni ai piani 2, 4 e 6.

## • VLAN 40

- In entrata: da VLAN 20, 30, 50, 60
- In uscita: verso le VLAN 30, 50, 60

Questa configurazione permette al piano 4 (amministrazione) di ricevere comunicazioni dai piani 2 (ufficio vendite), 3 (ufficio acquisti), 5 (dirigenza) e 6 (reparto IT) e di inviare informazioni ai piani 3, 5 e 6. Il piano amministrazione svolge quindi la funzione di tramite tra i piani dirigenziali e quelli operativi e viceversa.

## • VLAN 50

- In entrata: da VLAN 40 e 60
- In uscita: verso la VLAN 40

Questa configurazione permette al piano 5 (dirigenza) di ricevere comunicazioni dai piani 4 (amministrazione) e 6 (reparto IT) e di inviare informazioni al piano 4.

## • VLAN 60

- In entrata: dalle VLAN 30, 40
- In uscita: verso tutte le VLAN

Questa configurazione permette al piano 6 (reparto IT) di ricevere comunicazioni dai piani 3 (ufficio acquisti) e 4 (amministrazione) e di inviare informazioni a tutti i piani. Questo permette al reparto IT di effettuare manutenzione su tutti i dispositivi e di ricevere informazioni dai due snodi principali della rete (piani 3 e 4). Questo perché nel reparto IT troviamo un database aziendale a cui vengono inviate informazioni da archiviare.

# CONFIGURAZIONE DELLE ACL PER IL CONTROLLO DELLE COMUNICAZIONI TRA LE VLAN

The screenshot shows the CLI interface for Router4. The 'CLI' tab is selected. The command entered is 'Router#show access-lists'. The output displays six Extended IP access lists (101 to 106) configured to control traffic between VLANs. The lists include deny rules for specific source and destination IP ranges and permit rules for specific source and destination IP ranges.

```
ROUTER>enable
Router#show access-lists
Extended IP access list 101
 10 deny ip 192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255
 20 deny ip 192.168.10.0 0.0.0.255 192.168.60.0 0.0.0.255
 30 deny ip 192.168.10.0 0.0.0.255 192.168.80.0 0.0.0.255
 40 permit ip 192.168.10.0 0.0.0.255 192.169.15.0 0.0.0.255
 50 permit ip any any
Extended IP access list 102
 10 deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
 20 deny ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255
 30 deny ip 192.168.20.0 0.0.0.255 192.168.60.0 0.0.0.255
 40 deny ip 192.168.20.0 0.0.0.255 192.168.80.0 0.0.0.255
 50 permit ip any any
Extended IP access list 103
 10 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
 20 deny ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
 30 deny ip 192.168.30.0 0.0.0.255 192.168.80.0 0.0.0.255
 40 permit ip any any
Extended IP access list 104
 10 deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
 20 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
 30 permit ip any any
Extended IP access list 105
 10 deny ip 192.168.50.0 0.0.0.255 192.168.10.0 0.0.0.255
 20 deny ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255
 30 deny ip 192.168.50.0 0.0.0.255 192.168.30.0 0.0.0.255
 40 deny ip 192.168.50.0 0.0.0.255 192.168.60.0 0.0.0.255
 50 deny ip 192.168.50.0 0.0.0.255 192.168.80.0 0.0.0.255
 60 permit ip any any
Extended IP access list 106
 10 permit ip any any
Router#
Router#
```

Copy      Paste

Top

Entrando nel pratico, qui possiamo osservare le varie Access Lists configurate per il controllo delle comunicazioni tra le varie VLAN. Quindi come specificato precedentemente:

Queste regole NEGANO la comunicazione dal piano 2 verso i piani 4,5,6 e la DMZ. Permettendo la comunicazione con il piano 1 ed il piano 3.

Queste regole NEGANO la comunicazione dal piano 5 verso i piani 1,2,3,6 e la DMZ. Permettendo la comunicazione unicamente con il piano 4.

# LA ZONA DEMILITARIZZATA E I SERVER WEB E SMTP

La zona demilitarizzata (DMZ) è stata collegata tramite uno switch al firewall permettendo la connessione a Internet. Al suo interno, sono presenti i servizi pubblici dell'azienda, come il web server e il server SMTP. Questi server sono accessibili dall'esterno per garantire la disponibilità dei servizi aziendali, ma sono protetti dal firewall e configurati in modo da limitare l'accesso alle sole porte necessarie (80, 443, 25).



# SICUREZZA PERIMETRALE E GESTIONE DEL TRAFFICO

Il firewall perimetrale è stato configurato per proteggere la rete interna di Theta da minacce esterne. Si è deciso di disporre il dispositivo tra le tre interfacce principali di nostro interesse:

- Rete interna
- DMZ
- Rete esterna (internet)

Questo ci ha permesso di filtrare il traffico in tutte le direzioni, tramite le seguenti regole:

## Accesso alla DMZ

Accesso alla DMZ: Il firewall consente solo il traffico in ingresso sulle porte 80 (HTTP), 443 (HTTPS) e 25 (SMTP) diretto verso il web server e il server SMTP presenti nella DMZ. Questo permette l'accesso sicuro ai servizi web e di posta elettronica aziendali da parte di utenti esterni.

## Accesso alla rete interna

Nessun traffico diretto è consentito dall'esterno alla rete interna. Tuttavia, le risposte a richieste legittime generate dall'interno (ad esempio, quando un computer interno accede a un sito web) sonomesse.

## Filtraggio da DMZ a rete interna

Le comunicazioni sulla porta 23 (Telnet) tra la DMZ e la rete interna sono bloccate per evitare potenziali attacchi sfruttando questo protocollo non sicuro.

# ACCESS LISTS PER LA CONFIGURAZIONE DEL FIREWALL

The screenshot shows a window titled "Firewall" with tabs "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs, it says "IOS Command Line Interface". The interface displays system information and interface status messages:

```
bridging software.  
X.25 software, Version 3.0.0.  
5 Gigabit Ethernet/IEEE 802.3 interface(s)  
32K bytes of non-volatile configuration memory.  
63488K bytes of ATA CompactFlash (Read/Write)  
  
Press RETURN to get started!  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet8/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet7/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet9/0, changed state to up  
  
Router>enable  
Router#show access-lists  
Extended IP access list 120  
 10 deny tcp any 192.168.0.0 0.0.255.255 eq telnet  
 20 permit ip any 192.168.0.0 0.0.255.255  
 30 permit ip any any  
Extended IP access list 109  
 10 permit tcp any 192.168.80.0 0.0.0.255 eq www  
 20 permit tcp any 192.168.80.0 0.0.0.255 eq 443  
 30 permit tcp any 192.168.80.0 0.0.0.255 eq smtp  
 40 deny ip any 192.168.80.0 0.0.0.255  
 50 permit tcp any any established  
 60 deny tcp any any  
 70 deny udp any any  
  
Router#
```

At the bottom of the window are "Copy" and "Paste" buttons, and a "Top" checkbox.

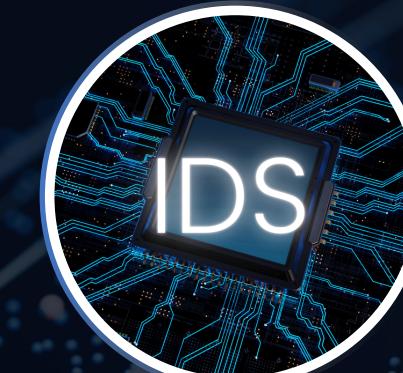
Sono le tre interfacce del Firewall dirette verso la rete interna, la DMZ e la rete esterna (internet)

Regola il traffico dalla DMZ alla rete

Regola il traffico verso la DMZ

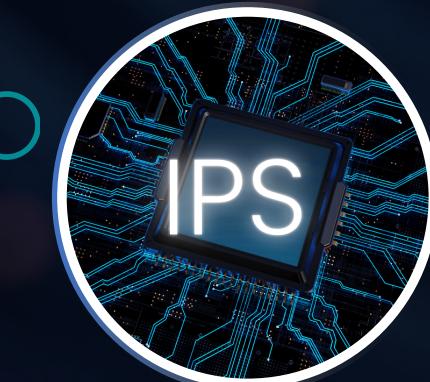
Regola il traffico dalla rete esterna alla rete interna

# DISPOSITIVI IDS/IPS



Tecnologia di sicurezza informatica avanzata che non solo rileva le intrusioni o attività sospette, ma è anche in grado di bloccarle o prevenirle in tempo reale. In caso di rilevamento, un IPS può eseguire azioni preventive, come il blocco del traffico sospetto.

Tecnologia di sicurezza informatica progettata per monitorare e analizzare il traffico di rete o le attività di sistema al fine di rilevare comportamenti sospetti o potenzialmente dannosi. Quando un'eventuale minaccia viene rilevata, l'IDS invia un allarme per avvisare gli amministratori di sistema.



### Posizionamento IPS:

- Integrato nel firewall Cisco ASA 5508-X, tra rete interna, DMZ e Internet.

### Funzioni IPS:

- Protezione multilivello da attacchi esterni e interni.
- Monitoraggio e controllo del traffico tra le zone.
- Isolamento dei servizi pubblici nella DMZ per evitare compromissioni.

### Motivazioni IDS:

- Rete inter-piano protetta senza rallentare la banda interna.
- Migliore visione integrata delle comunicazioni aziendali.
- IDS passivi evitano blocchi non necessari (meno falsi positivi rispetto a IPS).

### Distribuzione IDS:

- Switch 1 (Nodo centrale): Software IDS per monitoraggio del traffico iniziale.
- Switch 4 (Nodo centrale): Software IDS per monitoraggio traffico verso segmenti interni (Switch 5, 6 e Server).
- Switch 2, 3, 5, 6: Sensori IDS per analisi segmentata e rilevamento attacchi localizzati.



# POSSIBILI IMPLEMENTAZIONI

## REVERSE PROXY

Un reverse proxy agisce come un intermediario tra i client esterni e i server interni, ricevendo le richieste in ingresso e instradandole verso i server giusti.

L'azienda Security Griffins suggerisce l'installazione di un reverse proxy tra la DMZ e il firewall in quanto è una soluzione molto vantaggiosa per migliorare la sicurezza e la gestione del traffico nella rete aziendale.

## DATABASE

Questo server potrebbe ospitare database aziendali critici e migliorare la scalabilità e la gestione delle risorse per il futuro.

Consigliamo l'aggiunta di un server database nel reparto IT (piano 6) per migliorare la gestione dei dati aziendali. Inoltre, si consiglia di monitorare regolarmente la configurazione della rete e di aggiornare le regole firewall e le ACL per proteggere la rete da nuove minacce emergenti.

# RETE E FIREWALL

## RETE

rete interna: connette i dispositivi all'interno dell'azienda e non è accessibile dall'esterno senza configurazioni specifiche. Utilizza il WEB SERVER software o un dispositivo che ospita e distribuisce pagine web e applicazioni. Comunica attraverso il protocollo HTTP/HTTPS per rispondere alle richieste dei client (ad esempio i browser).

caratteristiche web server:

- facilità d'uso
- sicurezza
- accesso multi rete

## FIREWALL PFSENSE

Il firewall pfSense è stato configurato per proteggere la rete interna e gestire in modo flessibile le comunicazioni tra i diversi segmenti azienda

Regole di Firewall Personalizzate:

- Separazione delle Reti
- Filtri per il Web
- Regole di Accesso Basate su IP e Porte

Funzionalità Avanzate di pfSense:

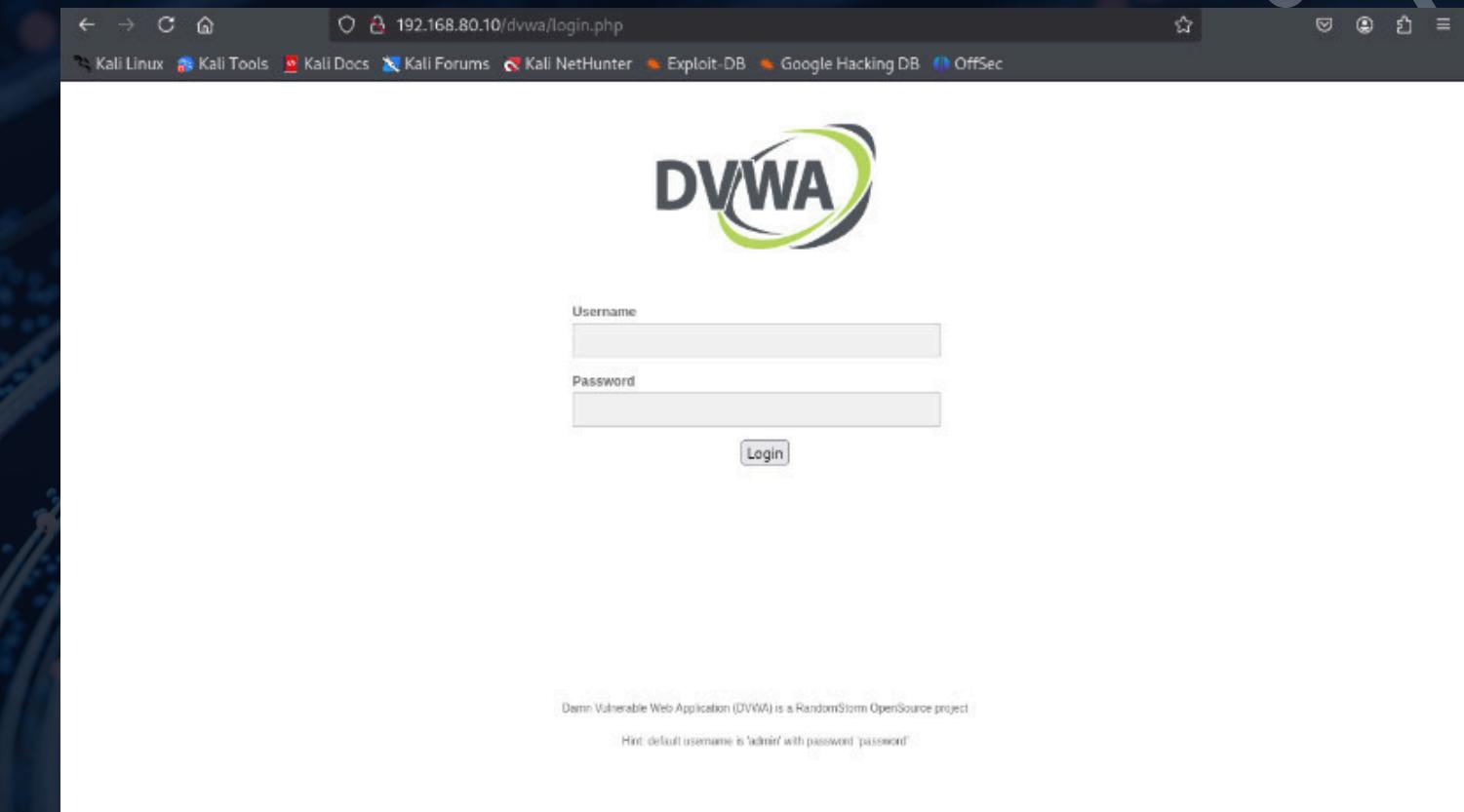
- VPN
- Intrusion Detection and Prevention System (IDS/IPS)
- Load Balancing e Failover

# RETE E FIREWALL

## WEB SERVER

Per verificare l'impianto e le sue possibili vulnerabilità ho eseguito diverse simulazioni tramite DVWA, che ho utilizzato esattamente come se fosse un webserver, alla ricerca delle possibili vulnerabilità della rete.

Di seguito allego il collegamento riuscito tra le due macchine che ho preso in esame.



```
(kali㉿kali)-[~/Desktop/BuildWeek-1/PortScanner/GuiHomePage]
$ ping 192.168.80.10
PING 192.168.80.10 (192.168.80.10) 56(84) bytes of data.
64 bytes from 192.168.80.10: icmp_seq=1 ttl=63 time=7.19 ms
64 bytes from 192.168.80.10: icmp_seq=2 ttl=63 time=2.60 ms
64 bytes from 192.168.80.10: icmp_seq=3 ttl=63 time=3.62 ms
64 bytes from 192.168.80.10: icmp_seq=4 ttl=63 time=4.51 ms
64 bytes from 192.168.80.10: icmp_seq=5 ttl=63 time=1.40 ms
64 bytes from 192.168.80.10: icmp_seq=6 ttl=63 time=1.67 ms
64 bytes from 192.168.80.10: icmp_seq=7 ttl=63 time=1.50 ms
64 bytes from 192.168.80.10: icmp_seq=8 ttl=63 time=2.37 ms
64 bytes from 192.168.80.10: icmp_seq=9 ttl=63 time=12.7 ms
64 bytes from 192.168.80.10: icmp_seq=10 ttl=63 time=17.4 ms
64 bytes from 192.168.80.10: icmp_seq=11 ttl=63 time=2.60 ms
64 bytes from 192.168.80.10: icmp_seq=12 ttl=63 time=1.65 ms
```

# RETE E FIREWALL

## SQUIDGUARD, SQUIDPROXY

Per quanto riguarda l'implementazione di regole mi sono fornito di due servizi aggiuntivi per il firewall , SquidGuard e SquidProxy.

Tramite questi due servizi sono riuscito ad implementare una regola che bloccasse degli specifici indirizzi malevoli, dato il path url di essi.

Di seguito potete vedere l'esempio.

Proxy filter SquidGuard: Target categories / Edit / Target categories

General settings Common ACL Groups ACL **Target categories** Times Rewrites Blacklist Log XMLRPC Sync

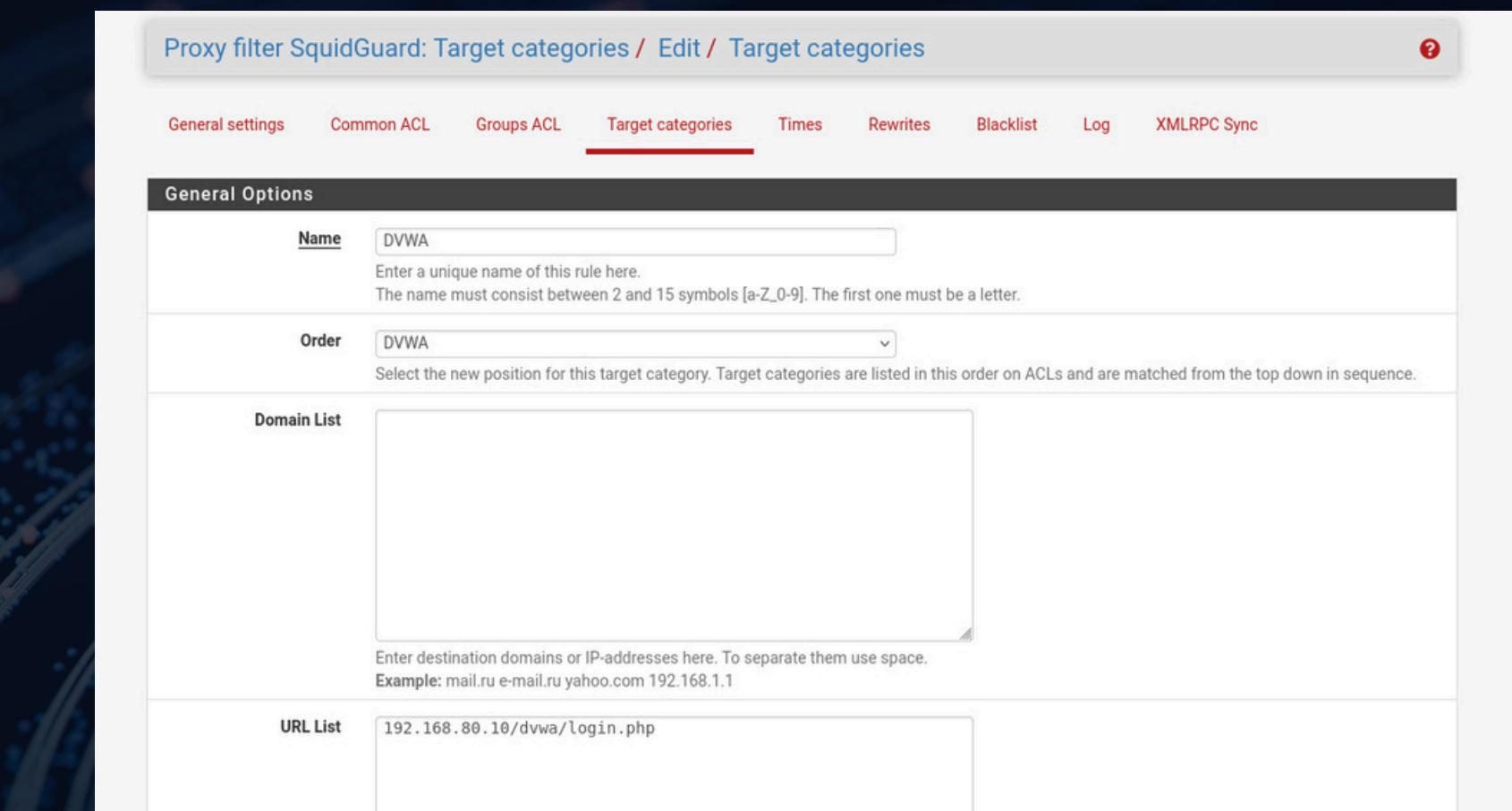
**General Options**

Name DVWA  
Enter a unique name of this rule here.  
The name must consist between 2 and 15 symbols [a-Z\_0-9]. The first one must be a letter.

Order DVWA  
Select the new position for this target category. Target categories are listed in this order on ACLs and are matched from the top down in sequence.

Domain List  
Enter destination domains or IP-addresses here. To separate them use space.  
Example: mail.ru e-mail.ru yahoo.com 192.168.1.1

URL List 192.168.80.10/dvwa/login.php



← → ⌂ ⌂ 192.168.80.10/dvwa/login.php  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-D



**Request denied by pfSense proxy: 403 Forbidden**

**Reason:**

**Client address:** 192.168.50.11  
**Client name:** 192.168.50.11  
**Client group:** default  
**Target group:** DVWA  
**URL:** http://192.168.80.10/dvwa/login.php

# PENTESTING

## PENTESTING

Il processo di pentesting viene utilizzato per identificare eventuali vulnerabilità nella rete. Dopo aver simulato diversi scenari di attacco, sono stati analizzati i seguenti aspetti

- Forza delle regole di firewall
- Robustezza del WebServer
- Protezione da phishing e malware

I risultati di questi test hanno portato a ulteriori ottimizzazioni delle regole del firewall e alla definizione di policy più restrittive.

## CONCLUSIONE

La rete interna di Theta è stata progettata per essere robusta, sicura e intuitiva. L'implementazione del firewall pfSense e del WebServer ha garantito:

- Una protezione completa contro attacchi esterni e rischi interni.
- Accesso controllato e sicuro alle risorse aziendali.
- Semplicità d'uso per i dipendenti, con una configurazione che consente di lavorare in ambienti diversi senza compromessi sulla sicurezza.

# HTTP REQUEST

## DEFINIZIONE:

Un HTTP request è una richiesta inviata da un client a un server per ottenere dati o eseguire azioni, usando il protocollo HTTP.

## UTILIZZO:

Serve per accedere a pagine web, inviare dati (es. moduli), scaricare file o interagire con API.

A screenshot of a terminal window titled "File Edit Search View Document Help" and "Desktop/BuildWeek-1/HTTPrequest/http\_requests\_logs/http\_requests\_log\_20241128\_162423.txt - Mousped". The window displays a log of 21 HTTP requests. The log includes details such as the date (Thu, 28 Nov 2024), time (11:56:18 GMT), server (Apache/2.2.8 (Ubuntu) DAV/2), X-Powered-By (PHP/5.2.4-2ubuntu5.10), Pragma (no-cache), Cache-Control (no-cache, must-revalidate), Expires (Tue, 23 Jun 2009 12:00:00 GMT), Set-Cookie (PHPSESSID=5ecf602fdf82b2db5b2dcda47a4a95e; path=/, security=high), Content-Length (1289), Keep-Alive (timeout=15, max=100), Connection (Keep-Alive), Content-Type (text/html; charset=utf-8), and Allowed Methods (Non specificati). The log also shows methods like GET, POST, and PUT, and status codes like 200 and 204.

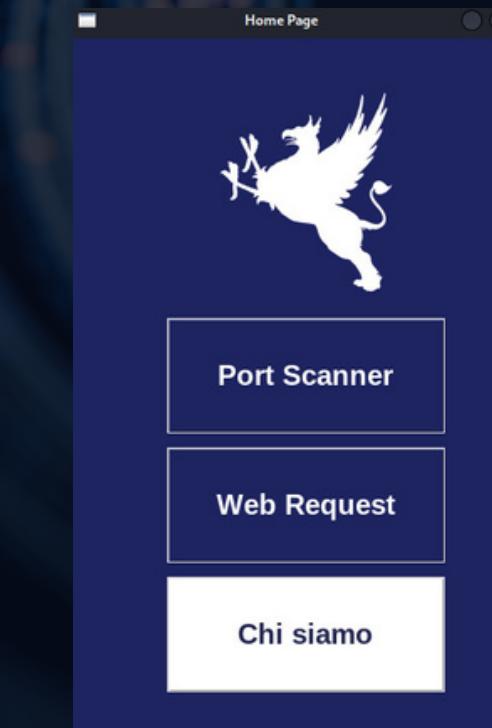
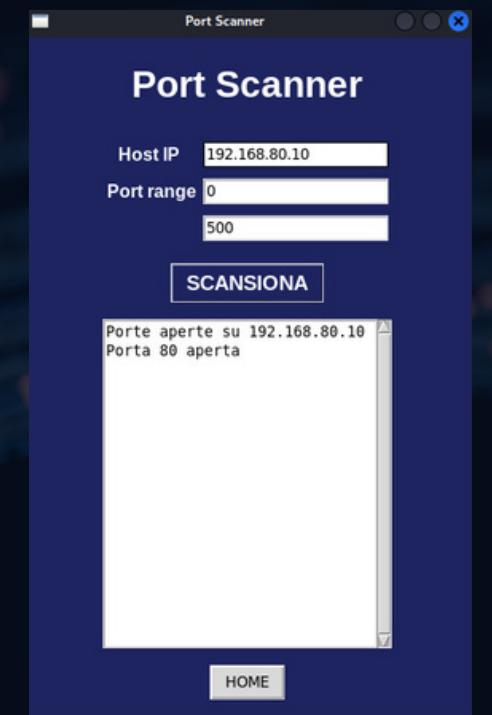
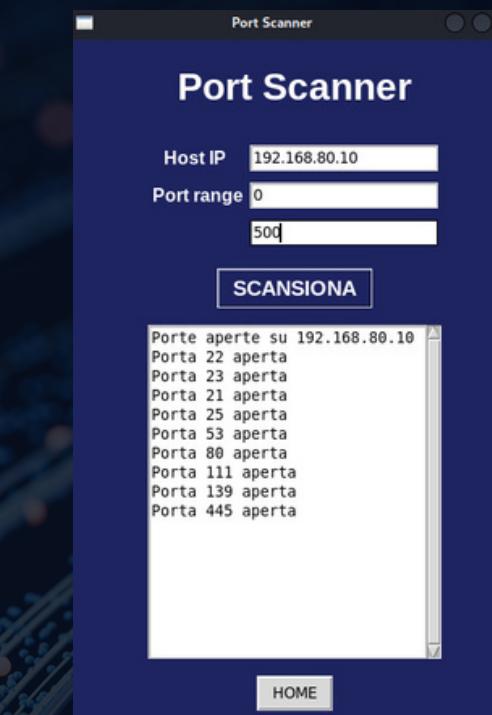
# PORTSCANNER

## DEFINIZIONE:

Un port scanner è uno strumento usato per analizzare le porte di un dispositivo connesso a una rete, identificando quali sono aperte, chiuse o filtrate.

## UTILIZZO:

- Valutare la sicurezza di un sistema, rilevando porte vulnerabili.
- Diagnosticare problemi di rete.
- Scoprire servizi attivi su un dispositivo (es. server web, database).



# SNIFFER

## DEFINIZIONE:

Strumento che cattura e analizza i pacchetti di dati in transito su una rete.

## UTILIZZO:

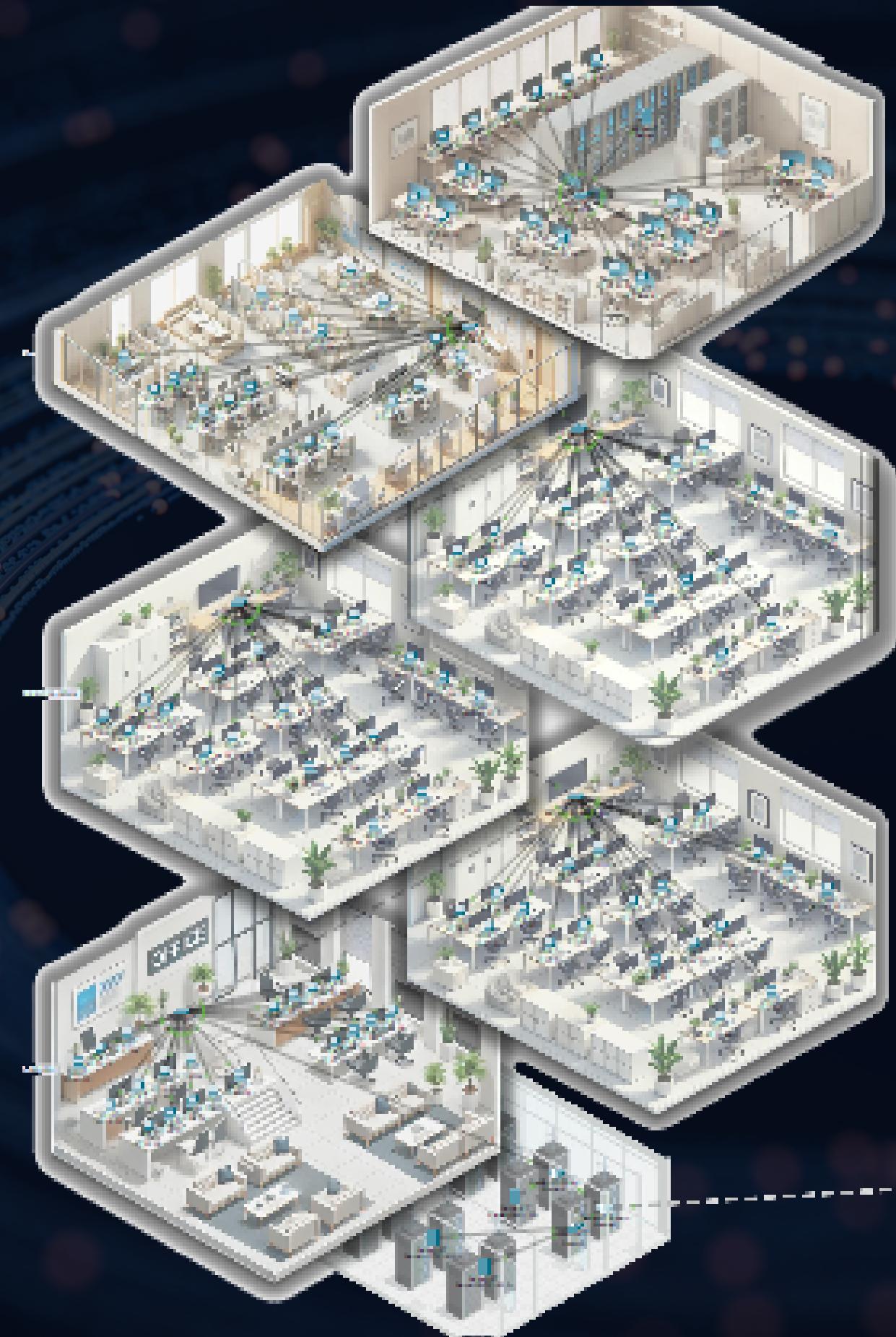
Utilizzato per monitorare, diagnosticare problemi, ottimizzare le prestazioni e rilevare minacce alla sicurezza. L'obiettivo può essere raggiunto in 2 casi principali:

- tramite utilizzo libreria socket
- tramite utilizzo libreria scapy

# PREVENTIVO

considerando i device migliori sul mercato e le licenze necessarie al corretto funzionamento delle componenti, si propone il seguente preventivo:

**55.304,46€**



# DEVICE FISICI

Il team ha deciso di proporre le seguenti componenti:

## ROUTER CISCO ISR 4331

Il router è un dispositivo di rete essenziale nella progettazione dell'infrastruttura di Theta. È responsabile della gestione del traffico tra le sottoreti interne (VLAN) e della connessione verso l'esterno tramite il firewall perimetrale.

Funzioni Principali:

- Inter-VLAN Routing
- Collegamento alla DMZ
- Access Control List (ACL)
- Collegamento al NAS
- Traffico verso l'esterno
- Qualità del Servizio (QoS)

Configurazione Tecnica di Riferimento

- Interfacce
- Indirizzamento IP:
- Protezione

Benefici dell'uso del Router

- sicurezza
- efficienza
- gestione centralizzata

## SWITCH CISCO C9200-24P-E

Gli switch sono i dispositivi fondamentali per la connettività a livello di piano. Ogni piano dell'edificio è dotato di uno switch dedicato che connette i computer e altri dispositivi della rete.

Funzioni principali:

- Connnettività a Livello di Piano
- Supporto VLAN
- Trunking verso il Router
- QoS (Qualità del Servizio)
- Sicurezza Locale

Configurazione Tecnica di Riferimento

- Porte
- VLAN

Benefici dell'uso dello Switch

- Scalabilità
- Segmentazione
- Flessibilità

## FIREWALL CISCO ASA 5508-X

Il firewall è il dispositivo chiave per la sicurezza perimetrale della rete aziendale di Theta. Si trova tra il router centrale e la connessione a Internet, e il suo ruolo principale è quello di filtrare il traffico, prevenire intrusioni e applicare politiche di sicurezza.

funzioni principali:

- Protezione della Rete Interna
- Accesso alla DMZ
- Filtraggio del Traffico Esterno
- Ispezione Stato-Connessione
- Gestione delle Regole

Configurazione Tecnica di Riferimento

- Interfacce
- Politiche

Benefici dell'uso del Firewall

- Sicurezza avanzata
- Controllo granulare
- Monitoraggio

# DEVICE FISICI

il team ha deciso di proporre le seguenti componenti:

## SERVER WEB

### DELL POWEREDGE T440

Server dedicato per l'hosting di applicazioni e pagine web. Fornire servizi HTTP (porta 80) e HTTPS (porta 443) agli utenti esterni.

Funzioni principali:

- Accesso Pubblico
- Protezione in DMZ
- Monitoraggio e Log

Benefici: sicurezza, affidabilità, isolamento

## SERVER SMTP

### DELL POWEREDGE T440

Server per la gestione della posta elettronica aziendale. Invio e ricezione di email tramite protocollo SMTP (porta 25).

Funzioni principali:

- Gestione Email
- Protezione in DMZ
- Filtri Anti-Abuso

Benefici: sicurezza, disponibilità isolamento

## SERVER NAS

### SYNOLOGY RACKSTATION RS2423+

Network Attached Storage per backup e condivisione di file. Archiviazione centralizzata e gestione dei backup aziendali.

Funzioni Principali

- Condivisione File
- Backup Dati
- Sicurezza

Benefici: Centralizzazione, efficienza: sicurezza

## SERVER DATABASE

### DELL POWEREDGE R650

Server dedicato per la gestione e l'archiviazione di dati strutturati

Funzioni Principali

- Gestione Dati
- Sicurezza
- Affidabilità

Benefici: Centralizzazione, efficienza, protezione

# LICENZE

il team ha deciso di proporre le seguenti licenze:

## Cisco ASA 5508-X VPN AnyConnect

Questa licenza permette una connessione sicura e affidabile per l'accesso remoto alla rete

Funzioni principali:

- Accesso VPN semplice e sicuro
- Autenticazione multi-fattore
- Gestione centralizzata

## Reverse Proxy NGINX

Riduce i tempi di risposta e ottimizza l'uso della rete.

Funzioni Principali:

- Bilancio del carico
- Caching
- Sicurezza avanzata
- Gestione dei protocolli

## Router ISR4331 Cisco DNA Center

Ottimizza la gestione delle reti aziendali centralizzando tutte le operazioni.

Funzioni Principali:

- Automazione della rete
- Visibilità analisi di rete
- Gestione della sicurezza

## Cisco Smart Net Total Care

Funzioni Principali:

- Offre supporto avanzato 24/7
- Aggiornamento software
- Patches di sicurezza
- Sostituzione hardware

## Cisco APPX

Funzioni Principali:

Ottimizza l'esperienza delle applicazioni garantendo prestazioni migliori.

- AVC (Application Visibility and Control)
- Wan Optimization
- APM (Application Performance Management)

## Switch Cisco C9200-24-P-E Cisco Network Avanzato

E' una soluzione ottimale per ottimizzare la rete.

Funzioni principali:

- Sicurezza avanzata di rete.
- Routing IPv4/IPv6
- QoS Avanzato
- Cisco StackWise-480



**Security Griffin ringrazia per l'attenzione  
Non vediamo l'ora di collaborare con voi**