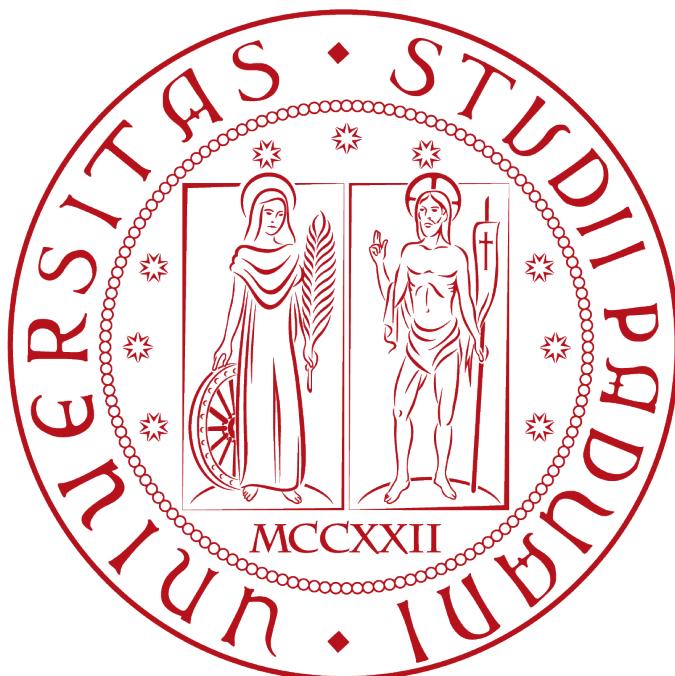


UNIVERSITÀ DEGLI STUDI DI PADOVA
DIPARTIMENTO DI MATEMATICA
”Tullio Levi-Civita”

Corso di Laurea in INFORMATICA



**Monitoraggio e sicurezza fisica di
Campus Area Network**

Tirocinante:	Mirco Cailotto, mat. 1123521
Relatore:	Dott. Paolo Baldan
Azienda Ospitante:	Wintech Spa
Tutor aziendale:	Roberto Pezzile

Anno Accademico 2017/2018

Ringraziamenti

Todo ringraziamenti.

Mirco Cailotto

Indice

Sommario

Convenzioni tipografiche

1	Contesto aziendale	1
1.1	Dominio applicativo	2
1.1.1	Digital Transformation	2
1.1.2	Applicazioni gestionali	2
1.1.3	Cloud	2
1.1.4	eLearning	2
1.1.5	Security	3
2	Progetto di stage	4
2.1	Panoramica del progetto	4
2.1.1	Obiettivi dello stage	5
2.1.2	Soluzioni e strumenti utilizzati	5
2.1.3	Problemi riscontrati	6
2.1.4	Risultati ottenuti	6
2.2	Struttura del documento di relazione	6
3	Pianificazione	7
3.1	Fase 1: Analisi	7
3.2	Fase 2: Progettazione	7
3.3	Fase 3: Implementazione	8
3.4	Fase 4: Test	8
3.5	Fase 5: Tuning	8
4	Obiettivi	10
4.1	Obiettivo aziendale	10
4.2	Obiettivo formativo	10
4.3	Risultati attesi	11

4.3.1	Monitoraggio	11
4.3.2	Gestione delle configurazioni dei dispositivi di rete	12
4.3.3	Politiche di sicurezza	12
4.3.4	Captive Portal	14
5	Tecnologie	15
5.1	Tecnologie per il monitoraggio	15
5.1.1	PRTG Network Monitor	15
5.1.2	Observium	16
5.1.3	RConfig	16
5.2	Tecnologie per la sicurezza	17
5.2.1	802.1X	17
5.2.2	Extensible Authentication Protocol	18
5.2.3	Windows Network Policy Server	18
5.2.4	Active Directory	19
5.2.5	CAPsMAN	19
5.3	Strumenti di lavoro	20
5.3.1	Microsoft Visio	20
5.3.2	OpenOffice Calc	20
5.3.3	GreaseMonkey	21
5.3.4	Putty	21
5.3.5	Microsoft Telnet	22
5.3.6	MySQL Command-Line Tool	22
5.3.7	Notepad++	22
5.3.8	Vim	23
5.3.9	FileZilla	23
6	Realizzazione	24
6.1	Analisi	24
6.1.1	Lista apparati	24
6.1.2	Analisi sistemi di sicurezza fisica	25
6.1.3	Analisi sistemi di monitoraggio	26
6.1.4	Schema di rete	26
6.2	Progettazione	28
6.2.1	Progettazione Observium	28
6.2.2	Progettazione rConfig	29
6.2.3	Progettazione della rete WiFi dedita agli uffici	30
6.2.4	Progettazione Captive portal	34
6.2.5	Progettazione entry DNS	38
6.2.6	Produzione della prima bozza della documentazione progettuale	38

6.3	Implementazione	39
6.3.1	Preparazione dell'ambiente	39
6.3.2	Configurazione del monitoraggio con Observium	40
6.3.3	Configurazione del versioning con RConfig	41
6.3.4	Configurazione nuovi apparati di rete	45
6.3.5	Attivazione servizio NPS in Active Directory	45
6.3.6	Creazione del Captive Portal	47
6.3.7	Inserimento regole Firewall	48
6.3.8	Test delle configurazioni in laboratorio	49
6.3.9	Aggiornamento della documentazione progettuale	51
6.4	Test finali	52
6.4.1	Individuazione problematiche	52
6.4.2	Aggiornamento della documentazione progettuale	53
6.5	Tuning	54
6.5.1	Upgrade Observium	54
6.5.2	Allarmi Observium tramite E-mail e Telegram	55
6.5.3	Raggruppamento delle interfacce	57
6.5.4	Raggruppamento dispositivi	57
6.5.5	Completamento della documentazione	57
7	Valutazione retrospettiva	58
7.1	Tempo impiegato	58
7.1.1	Riepilogo tempo impiegato	58
7.1.2	Considerazioni sugli scostamenti	58
7.2	Risultati ottenuti	59
7.2.1	Soddisfacimento risultati attesi	59
7.2.2	Risultati aziendali	62
7.2.3	Sviluppi futuri	63
7.2.4	Risultati personali	63
7.3	Vincoli del progetto	65
7.3.1	Vincoli tecnologici	65
7.3.2	Vincoli temporali	66
Appendici		68
Appendice A:	Schemi di rete	68
Appendice B:	Script di popolamento rConfig	72
Appendice C:	Script di backup Mikrotik	75
Glossario		77

INDICE

Bibliografia	80
Documenti in lingua italiana	80
Documenti in lingua inglese	80

Elenco delle figure

1.1	Logo di Wintech	1
5.1	Logo di PRTG	15
5.2	Logo di Observium	16
5.3	Schema delle iterazioni tra i dispositivi secondo 802.1X	17
5.4	Procedura di autenticazione 802.1X	18
5.5	Interfaccia di Visio	20
5.6	Interfaccia di Calc	20
5.7	Logo di GreaseMonkey	21
5.8	Schermata iniziale di Putty	21
5.9	Interfaccia di Notepad++	22
5.10	Interfaccia di Vim	23
5.11	Logo di FileZilla	23
6.1	Schermata di PRTG Network Monitor	26
6.2	Interfacce visualizzate all'interno di Observium	29
6.3	Attacco SQL injection su rConfig, sulla destra tutte le configurazioni navigabili	30
6.4	Schema dei dispositivi e dei protocolli usati per le reti Corporate e Mobile	32
6.5	Schema dei dispositivi e dei protocolli usati per la rete Guest	33
6.6	Schermata per la richiesta di un account	34
6.7	Sequenza per effettuare il login	36
6.8	Sequenza per effettuare la registrazione	37
6.9	Switch HP 2530-8G PoE+	40
6.10	Access Point MikroTik cAP ac	40
6.11	Controller MikroTik	40
6.12	Esempio della scarsa normalizzazione dei dati in rConfig	43
6.13	Lista delle cartelle con i backup in Directory Lister	44
6.14	Configurazione della rete	45
6.15	Politiche di sicurezza utilizzate	46

ELENCO DELLE FIGURE

6.16 Configurazione RADIUS del controller MikroTIk	46
6.17 Risultato ottenuto dalla analisi di VEGA	49
6.18 Risultati ottenuti con NetCut	50
6.19 Alert checks creati in Observium	55
6.20 Screenshot degli avvisi nell'applicazione Telegram	56
6.21 Stato dell'utilizzo del ponte radio	57
7.1 Schema Visio della rete datato 2015	69
7.2 Schema Visio della rete a fine stage, prima parte	70
7.3 Schema Visio della rete a fine stage, seconda parte	71

Elenco delle tabelle

4.1	Risultati attesi per l'implementazione di Observium	11
4.2	Risultati attesi per l'implementazione di rConfig	12
4.3	Risultati attesi per l'implementazione delle politiche di sicurezza . .	13
4.4	Risultati attesi per l'implementazione del Captive Portal	14
6.1	Servizi per l'implementazione del Captive Portal	48
7.1	Tempo previsto ed impiegato	58
7.2	Risultati ottenuti per l'implementazione di Observium	59
7.3	Risultati ottenuti per l'implementazione di rConfig	59
7.4	Risultati ottenuti per l'implementazione delle politiche di sicurezza	60
7.5	Risultati ottenuti per l'implementazione del Captive Portal	61

Sommario

Questo documento si prefigge lo scopo di presentare il lavoro svolto durante l'attività di stage, presso Wintech Communications Factory.

Le attività sono state intraprese nell'ambito sistemistico, andando a monitorare e a migliorare la sicurezza di una Campus Area Network di elevata complessità.

Con l'avanzamento delle nuove tecnologie succede sempre più di frequente che le aziende debbano estendere la propria rete, incrementandone la complessità e quindi le possibili problematiche, le quali devono essere correttamente controllate e gestite.

L'attività svolta ha riguardo il controllo in tempo reale dello stato di una rete di dimensioni considerevole, al fine di individuare colli di bottiglia, problematiche di varia natura e potenziali pericoli, permettendo di intervenire in modo tempestivo o preventivo.

L'attenzione sarà posta anche sul disaster recovery in caso di guasti dei dispositivi, salvando periodicamente tutte le configurazioni in uso, in modo tale da permettere una sostituzione rapida degli apparati.

Ulteriormente verrà trattata la sicurezza fisica delle reti, impedendo un accesso non autorizzato a risorse di elevata criticità mediante connessione Wi-Fi a coloro che non possiedono dei privilegi sufficientemente elevati.

Convenzioni tipografiche

Per favorire la lettura del documento e la sua comprensione è stato introdotto un glossario.

Qualora un termine presente nel glossario comparisse all'interno del testo, in un contesto nel quale si suppone il lettore possa non comprenderlo, verrà evidenziato rispetto al paragrafo presentandolo scritto in corsivo e apponendogli in conclusione una "G" al pedice.

Nel caso si stesse visionando la versione digitale di questo documento è possibile essere reindirizzati direttamente al termine nel glossario semplicemente cliccandoci sopra.

Capitolo 1

Contesto aziendale

Nata nel 1987, Wintech Comumnication Factory SPA è ad oggi uno dei pochi *System Integrator* capace di vantare una lunga tradizione e un patrimonio di conoscenze nei diversi ambiti di competenza del settori ICT.

WinTech Spa svolge la propria attività in qualità di System Integrator che, grazie alla propria esperienza, competenza e creatività, trasforma le tecnologie IT di mercato in soluzioni informatiche innovative, efficienti e dal facile utilizzo.



Figura 1.1: Logo di Wintech

La società conta su una struttura di circa 80 risorse che svolgono la propria attività nelle Sedi di Padova, Milano, Bassano del Grappa e Pordenone; una precisa strategia di valorizzazione di partnership nazionali ed internazionali, le consente di superare i confini delle proprie dimensioni fruendo di collaborazioni di valore riconosciuto.

1.1 Dominio applicativo

Wintech opera in un dominio molto vasto, per tale motivo in questa sezione verrà trattato con maggiore dettaglio il dominio relativo allo stage svolto, cioè quello del monitoraggio e della sicurezza fisica delle reti.

1.1.1 Digital Transformation

La trasformazione digitale è quell'insieme di cambiamenti nei comportamenti aziendali e di business collegato e veicolato dalla tecnologia digitale, tramite la quale è possibile traguardare una maggiore competitività di mercato.

Wintech si impegna in questo settore favorendo la digitalizzazione delle aziende, andando ad integrare sistemi che consentano una archiviazione elettronica dei documenti, certificati mediante firme digitali.

Ulteriormente si impegna anche a fornire soluzioni di Business Process Management e di Case Management, permettendo quindi una gestione evoluta di tutti i processi aziendali.

1.1.2 Applicazioni gestionali

Per consentire la gestione delle risorse aziendali Wintech propone soluzioni dedicate di Enterprise Resource Planning, Business Intelligence e di tesoriere.

Questi software, complementare tra di loro, permettono di monitorare, analizzare e accedere alle risorse disponibili in modo efficace ed efficiente, portando quindi enormi benefici alle aziende che ne fanno uso.

1.1.3 Cloud

Wintech offre servizi cloud mirati alle aziende e certificati secondo lo standard ISO 27001.

I vantaggi offerti da questa esternalizzazione è un supporto professionale e continuo dei propri sistemi, affiancato da una riduzione del downtime grazie al servizio ridondante ad alta affidabilità ed a una sicurezza elevata che protegge le risorse da intrusioni esterne.

1.1.4 eLearning

Wintech desidera migliorare anche la fruizione dei corsi aziendali, operando nello sviluppo di nuove tecnologie che ne consentano un utilizzo da remoto mantenendone la validità legale e assicurando la presenza fisica dell'interessato al terminale

durante le lezioni.

Questo viene effettuato mediante piattaforme di eLearning e di Live Streaming, integrate con software avanzati che consentono funzionalità non presenti nella concorrenza.

1.1.5 Security

Evoluzione della Cybersecurity

L'ambito della Cybersecurity è sicuramente uno degli ambiti più dinamici all'interno del mondo informatico, con tipologie di attacchi che variano continuamente nel tempo. Questo può essere riscontrato analizzando i vettori di attacco, chiaramente descritti anche annualmente all'interno del rapporto Clusit.

Oramai è inutile chiedersi se si verrà attaccati, ma ci si deve chiedere solamente quando succederà e se si è pronti a difendersi ed a riparare ai possibili danni. Praticamente qualsiasi ente è un potenziale bersaglio ed, a volte, espone delle vulnerabilità delle quali non si preoccupa, in quanto suppone erroneamente di non essere appetibile per un eventuale attaccante.

A sostegno di quanto appena affermato viene utilizzato, nel mondo anglosassone, il seguente motto:

Is not a matter of "if", but a matter of "when".

Il quale può essere tradotto in italiano nel seguente modo:

Non è una questione di "se", ma di "quando".

In conclusione bisogna sfatare l'immaginario collettivo in cui siano solo le grandi società americane, grandi brand, ad essere attaccate per attivismo. Le motivazioni sono notevolmente mutate e hanno come target qualsiasi azienda, anche le realtà della piccole e medie imprese che costituiscono il tessuto delle aziende italiane sono pesantemente bersagliate.

La proposta di Wintech in ambito Cybersecurity

La proposta per consentire di mantenere un elevato livello di sicurezza all'interno delle proprie reti proposto da Wintech si compone di svariate tecnologie, che vanno ad integrarsi per permettere una protezione completa su tutti i possibili fronti di attacco.

Le tecnologie illustrate in questo documento sono una parte di quelle utilizzate all'interno dell'azienda, mirate al monitoraggio della rete, al controllo della configurazione degli apparati ed al port-based Network Access Control.

Capitolo 2

Progetto di stage

Lo scopo dell'attività di stage è l'analisi, la progettazione e l'implementazione di un sistema di monitoraggio e di nuove politiche di sicurezza relative a una LAN Campus.

Le conoscenze apprese durante lo svolgimento dell'attività consistono nella capacità di progettare ed implementare una soluzione per raggiungere gli obiettivi prefissati, oltre che ad effettuare attività di tuning per perfezionarla.

2.1 Panoramica del progetto

Il progetto di stage è costituito principalmente da tre parti:

- Sistema di monitoraggio;
- Sistema di versionamento delle configurazioni;
- Nuove politiche di sicurezza fisica.

Il sistema di monitoraggio avrà il compito di mantenere costantemente la rete sotto osservazione, notificando quando si presentano problemi.

Il sistema di versionamento delle configurazioni degli apparati di rete deve consentire una sostituzione fulminea in caso di guasti dell'infrastruttura, consentendo di ripristinare tutte le impostazioni presenti senza doverle ridefinire nuovamente.

Per terminare verrà sviluppato un sistema di autenticazione ad una rete WiFi che impedisca un accesso fisico alle risorse collegate per coloro che non ne possiedono i relativi privilegi.

2.1.1 Obiettivi dello stage

Il progetto di stage ha come obiettivo quello di risolvere alcune problematiche riscontrate dal cliente all'interno della propria rete.

Il primo problema è la presenza di un controllo non soddisfacente della rete, che non consente di individuare svariate problematiche finché esse non degenerano in un disservizio.

Anche le procedure di disaster recovery in caso di guasto dei dispositivi non erano adeguate, in quanto non esisteva nessun backup o indicazione della configurazione utilizzata, quindi in caso di guasto si doveva configurare da zero il nuovo apparato, identificando le periferiche connesse seguendo i cavi.

L'ultima problematica individuata è la rete Wireless presente negli uffici, protetta unicamente da una unica password che veniva a volte fornita agli ospiti e, senza autorizzazione, utilizzata anche per i dispositivi personali dei dipendenti. La situazione veniva aggravata dal fatto che la rete in esame fornisce l'accesso a risorse di elevata importanza, che non possono essere isolate in quanto utilizzate per lo svolgimento dell'attività lavorativa.

2.1.2 Soluzioni e strumenti utilizzati

Per implementare il monitoraggio si è scelto un software denominato Observium, che è andato ad affiancare ed in larga parte a sostituire un precedente servizio denominato PRTG Monitor.

Il software scelto per la raccolta automatica delle configurazioni è stato RConfig, che però ha presentato alcune problematiche nella sua implementazione con i dispositivi MikroTik. Questo ha richiesto lo sviluppo di uno script aggiuntivo da caricare sui dispositivi stessi per ottenere il risultato desiderato.

Per garantire una sicurezza fisica si è scelto di usufruire del protocollo di autenticazione 802.1X, che è stato appositamente sviluppato a questo fine.

La rete WiFi è stata implementata utilizzando il protocollo CAPsMAN in modo tale da favorirne l'estensione e la gestione, collegata a dei servizi NPS e Free-RADIUS per verificare l'autenticazione. È stato necessario anche sviluppare un piccolo Captive Portal, al fine di consentire la registrazione ad eventuali ospiti.

2.1.3 Problemi riscontrati

Durante l'attività di stage sono state incontrate alcune difficoltà e limitazioni tecniche, che hanno protratto il tempo impiegato in alcune attività. La più critica è stata l'impossibilità per RConfig di leggere autonomamente la configurazione dei dispositivi prodotti da MikroTik, che ha richiesto uno sviluppo di uno script dedicato non previsto inizialmente.

2.1.4 Risultati ottenuti

Al termine dell'attività di stage tutte le problematiche inizialmente rilevate sono state risolte.

Il sistema di monitoraggio mediante Observium e il versionamento delle configurazioni realizzato con RConfig e script sono stati completati con successo, permettendo quindi di prevenire eventuali problematiche e, nel caso che ciò non fosse possibile, intervenire con rapidità.

Le modalità di accesso alla rete WiFi degli uffici è stata completamente riprogettata, suddividendo gli utenti in tre gruppi in base al loro ruolo, i quali presentano anche modalità di autenticazioni diverse. Le risorse sono state rese disponibili unicamente per la categoria di persone che ne hanno necessità e sono protette dallo standard 802.1X, che ne garantisce la segregazione fino ad una corretta autenticazione dell'utente.

2.2 Struttura del documento di relazione

Questo documento è stato strutturato in più parti, che analizzano e ripercorrono tutto il progetto.

La prima parte introduce l'azienda presso la quale si è svolta l'attività di stage e il progetto di stage a grandi linee.

Successivamente viene presentata la pianificazione delle attività e gli obiettivi che si mira a raggiungere, analizzando anche le tecnologie utilizzate per raggiungerli.

La parte più consistente è la realizzazione, che descrive i compiti conseguiti per il soddisfacimento degli obiettivi prefissati.

La relazione si conclude con una valutazione retrospettiva dell'attività, nella quale viene analizzato lo scostamento temporale rispetto alla pianificazione, vengono presentati i risultati ottenuti e i vincoli che ho incontrato.

Capitolo 3

Pianificazione

Le attività sono state suddivise in cinque fasi principali, le quali hanno coperto tutta la durata del percorso formativo stabilito.

3.1 Fase 1: Analisi

- **Periodo previsto:** dal 04/06/2018 al 08/06/2018;
- **Numero di ore previste:** 40h.

L’obiettivo di questa prima fase del percorso è stata la familiarizzazione con l’infrastruttura amministrata da Wintech e con i supporti hardware e software da utilizzare per la realizzazione del progetto.

Sono stati analizzati lo schema di rete dell’infrastruttura, la lista degli apparati e delle loro caratteristiche, il sistema di sicurezza fisica e il sistema di monitoraggio presenti.

3.2 Fase 2: Progettazione

- **Periodo previsto:** dal 11/06/2018 al 22/06/2018;
- **Numero di ore previste:** 40h.

Nella seconda fase si è proceduto alla configurazione del software di monitoraggio Observium e del software di gestione della versione rConfig.

Per facilitare le attività è stata definita la nomenclatura da dare ai dispositivi.

Inoltre si è proceduto alla definizione delle logiche di sicurezza che sono state implementate basate sul protocollo 802.11X.

Durante questa fase è anche stata prodotta la prima bozza della documentazione progettuale.

3.3 Fase 3: Implementazione

- **Periodo previsto:** dal 25/06/2018 al 06/07/2018;
- **Numero di ore previste:** 80h.

In questa fase è stata implementata la nuova infrastruttura e sono stati resi operativi i software precedentemente configurati.
È stato creato un laboratorio con uno nuovo switch sul quale sono state testate le politiche precedentemente scelte per valutarne l'efficacia.

Una volta accertata la validità del nuovo sistema si è proceduto alla creazione delle configurazioni per tutti gli switch comprendenti la nuova politica di sicurezza e la loro installazione.

Successivamente i dispositivi sono stati inseriti all'interno del DNS e si sono resi operativi i software Observium e RConfig.

Durante questo periodo la documentazione progettuale è aggiornata in conseguenza alle attività svolte.

3.4 Fase 4: Test

- **Periodo previsto:** dal 09/06/2018 al 13/07/2018;
- **Numero di ore previste:** 40h.

La fase di test è la più importante perché è stato messo alla prova l'intero sistema con il picco dell'utenza.

L'attività svolta è stata il monitoraggio di eventuali anomalie, per poi censirle, cercare la fonte del problema, identificare una soluzione ed implementarla.

Durante questo periodo la documentazione progettuale è aggiornata in conseguenza alle attività svolte.

3.5 Fase 5: Tuning

- **Periodo previsto:** dal 16/07/2018 al 27/07/2018;
- **Numero di ore previste:** 80h.

Nella fase finale del progetto sono stati eseguiti tuning su tutta la rete, ove possibile, sia sugli apparati che nelle configurazioni dei software.

Questa attività è stata supportata dal software Observium, che nel frattempo avrà raccolto una mole di dati tale da permettere uno studio dei miglioramenti effettuabili.

Un'altra attività derivante dallo studio dei dati raccolti è stata la configurazione delle soglie di allarme automatici, i quali verranno comunicati tramite messaggio E-mail e Telegram.

In questa ultima fase si è proceduto anche a completare la documentazione.

Capitolo 4

Obiettivi

4.1 Obiettivo aziendale

L'obiettivo a fine stage è aumentare la sicurezza fisica e consentire il monitoraggio dello stato di una rete Campus Area Network dove accedono migliaia di persone.

La finalità è rilevare eventuali anomalie e colli di bottiglia presenti ed impedire l'uso illecito e non controllato dei servizi di rete, manipolazione delle informazioni e furto di dati.

Questo comprende l'implementazione e l'utilizzo di servizi e protocolli avanzati per ottenere e mantenere le migliori performance possibili garantendo anche una sicurezza elevata.

4.2 Obiettivo formativo

L'obiettivo per il tirocinante è acquisire competenze in ambito networking e security in un contesto reale quale una Campus Area Network estesa, variegata e con un numero di utenti elevato.

Questo al fine di permettere di mettere in pratica le conoscenze acquisite durante lo svolgimento dei corsi universitari e fornire uno stimolo ad approfondire ancora di più queste tematiche.

4.3 Risultati attesi

Di seguito sono indicati i risultati attesi, che dovranno essere soddisfatti durante le attività di stage.

Questi valori sono stati scelti in comune accordo tra il tutor aziendale ed il cliente, considerando la natura e l'estensione della rete.

4.3.1 Monitoraggio

Misurazione	Valore minimo accettato	Valore massimo accettato
Tempo medio di composizione di una pagina	0ms	500ms
Numero di dispositivi di rete monitorati in contemporanea	80	-
Numero di interfacce monitorate in contemporanea	2500	-
Numero di sensori e periferiche monitorati in contemporanea	500	-
Numero di alert checks presenti	10	20
Protezione delle informazioni tramite password	Si	-

Tabella 4.1: Risultati attesi per l'implementazione di Observium

Il numero di dispositivi presenti sono stati decretati in modo tale da riuscire a monitorare efficacemente la rete presente.

Gli alert check individuano le situazioni considerate pericolose, il loro numero è stato scelto in modo tale da permettere una individuazione precisa della problematica senza però aggiungere troppa verbosità.

4.3.2 Gestione delle configurazioni dei dispositivi di rete

Misurazione	Valore minimo accettato	Valore massimo accettato
Tempo di composizione di una pagina	0ms	200ms
Numero di dispositivi di rete gestiti in contemporanea	80	-
Protezione delle informazioni tramite password	Si	-

Tabella 4.2: Risultati attesi per l'implementazione di rConfig

Il tempo di composizione di una pagina concesso è inferiore rispetto a quello del monitoraggio in quanto le informazioni presenti all'interno del sistema sono inferiori numericamente, quindi il tempo necessario per visualizzarle dovrà essere inferiore.

4.3.3 Politiche di sicurezza

Misurazione	Valore richiesto
Possibilità per gli impiegati di usufruire dei servizi locali alla rete (stampanti, fax)	Si
Possibilità per gli impiegati di usufruire dei servizi remoti (accesso ai database, relay email)	Si
Possibilità per gli impiegati di accedere ad internet attraverso protocolli definiti	Si
Possibilità per i dispositivi mobili del personale di usufruire dei servizi locali alla rete (stampanti, fax)	No
Possibilità per i dispositivi mobili del personale di usufruire dei servizi remoti (accesso ai database, relay email)	No
Possibilità per i dispositivi mobili del personale di accedere ad internet attraverso qualsiasi protocollo	No
Possibilità per i dispositivi mobili del personale di accedere ad internet attraverso i protocolli HTTP, HTTPS, SMTP, SMTPTS, POP3, POP3S, IMAP, IMAPS, IPSEC VPN	Si

Misurazione	Valore richiesto
Necessità per i dispositivi mobili di effettuare una autenticazione tramite Captive Portal	No
Possibilità per gli ospiti di usufruire dei servizi locali alla rete (stampanti, fax)	No
Possibilità per gli ospiti di usufruire dei servizi remoti (accesso ai database, relay email)	No
Possibilità per gli ospiti di accedere ad internet attraverso qualsiasi protocollo	No
Possibilità per gli ospiti di accedere ad internet attraverso i protocolli HTTP, HTTPS, SMTP, SMTPL, POP3, POP3S, IMAP, IMAPS, IPSEC VPN	Si
Necessità per gli ospiti di effettuare una autenticazione tramite Captive Portal	Si

Tabella 4.3: Risultati attesi per l'implementazione delle politiche di sicurezza

Le modalità di accesso alla rete sono state scelte in modo tale da bilanciare sicurezza ed usabilità, considerando anche le modalità di utilizzo della rete da parte dei relativi fruitori.

4.3.4 Captive Portal

Misurazione	Valore richiesto
Possibilità di effettuare il login	Si
Possibilità di registrazione tramite sponsor	Si
Registrazione valida per un determinato periodo di tempo	Si
Interfaccia utilizzabile da un dispositivo mobile	Si
Registrazione tramite e-mail	Si
Possibilità di registrazione con e-mail altrui	No
Sezione di amministrazione facilmente accessibile	Si
Sezione di amministrazione protetta da password	Si
Funzionalità di gestione degli sponsor	Si
Funzionalità di gestione degli account	Si
Funzionalità di gestione delle durate temporali	Si

Tabella 4.4: Risultati attesi per l'implementazione del Captive Portal

I requisiti scelti sono stati decretati sulla base di soluzioni simili adottate da Win-tech S.P.A. e poi adattati alle esigenze del cliente

Capitolo 5

Tecnologie

Questa sezione illustra le principali tecnologie incontrate ed utilizzate nel corso dello stage per il controllo, il monitoraggio e la sicurezza delle reti di loro competenza.

Essendo la sicurezza informatica un settore nel quale gli standard, le leggi e le tipologie di attacco evolvono molto in fretta, le tecnologie utilizzate devono adeguarsi di conseguenza. Questo porta i tool ed i programmi utilizzati a diventare velocemente obsoleti oppure a variare con il passare del tempo.

5.1 Tecnologie per il monitoraggio

5.1.1 PRTG Network Monitor

PRTG è un sistema di monitoraggio della rete utilizzato nella rete analizzata durante lo stage. Il suo fine è la rilevazione delle anomalie, ma a causa delle limitazioni della versione gratuita e del suo elevato costo si è scelto di sostituirlo.

Il software consiste in un servizio al quale ci si collega mediante il client fornito oppure attraverso una interfaccia web e permette di tenere sotto controllo anche siti web e servizi di varia natura.

Questo software era già presente all'interno del sistema ed è stata analizzato durante la prima fase dello stage.



Figura 5.1: Logo di PRTG

5.1.2 Observium

Observium è un sistema di monitoraggio della rete compatibile con i dispositivi delle principali aziende produttrici di apparati di rete.

La sua implementazione durante l'attività formativa è stata effettuata per superare ai limiti posti da PRTG e migliorare quindi la qualità dei servizi.

Tra i dispositivi supportati si possono citare Cisco, Dell, HP, Huawei, Lenovo, MikroTik, Netgear e ZTE.

Il software dispone anche di una ricerca automatica dei dispositivi presenti all'interno della rete, funzionalità utile per reti di piccola-media dimensione.

Le funzionalità che fornisce sono il monitoraggio del *Quality Of Service*, il raggruppamento dei dispositivi mediante regole definite dall'utente e l'alert automatico nel caso vengano superate determinate soglie.

Questa tecnologia è stata implementata durante lo svolgimento dell'attività di stage.



Figura 5.2: Logo di Observium

5.1.3 RConfig

Il tool RConfig è un configuration management mirato ai dispositivi di rete che permette in modo veloce ed automatizzato di effettuare una copia delle configurazioni degli apparati di rete.

È completamente open source, protetto da licenza GNU v3.0, ed è scritto in linguaggio PHP. Per eseguire automaticamente i task fa uso del demone Unix crontab, quindi non risulta utilizzabile su sistemi Windows, ma unicamente Linux e BSD. Le connessioni verso i dispositivi non sono effettuate tramite lo standard Simple Network Management Protocol, o SNMP, ma Telnet e SSH. Questo gli permette di supportare, con la giusta configurazione, molti dispositivi, però complica notevolmente la fase di setup e può generare problemi in alcuni brand.

Questa tecnologia è stata implementata durante lo svolgimento dell'attività di stage.

5.2 Tecnologie per la sicurezza

5.2.1 802.1X

Il 802.1X è uno standard IEEE per il controllo di accesso alla rete port-based, parte della famiglia di protocolli IEEE 802.1. Fornisce un meccanismo di autenticazione mediante una combinazione username/password oppure un certificato digitale.

I dispositivi utilizzati in questo protocollo sono tre: il dispositivo di un utente, che richiede l'accesso alla rete, l'Autenticator, che comunica con il dispositivo, e un Authentication Server, che riceve la richiesta di accesso del dispositivo dall'Autenticator e decreta se approvarla o meno.

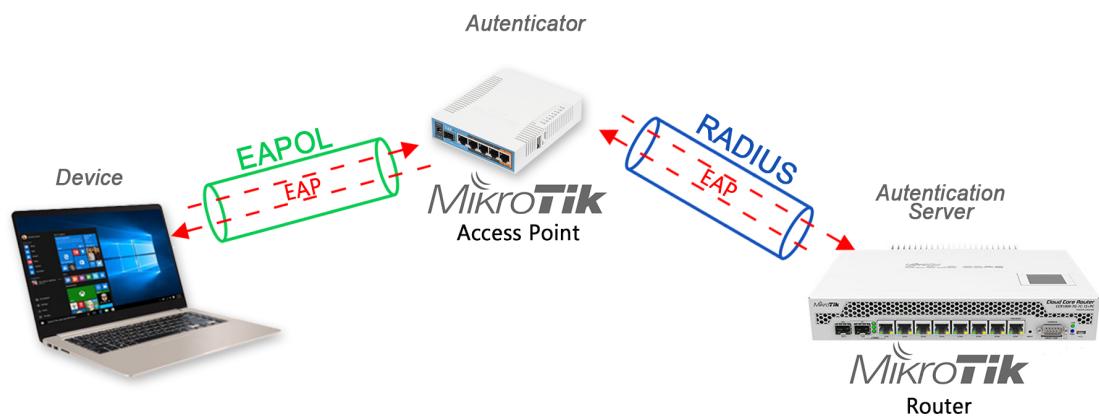


Figura 5.3: Schema delle iterazioni tra i dispositivi secondo 802.1X

La sua caratteristica principale è l'isolamento del dispositivo dalla rete durante la fase di autenticazione, impedendogli di interagire direttamente con qualsiasi altro dispositivo che non sia il Autenticator, il quale controllerà la validità dei messaggi ricevuti secondo il protocollo utilizzato per poi contattare il Authentication Server.

Questa protezione va ad ampliare la *sicurezza fisica* delle risorse connesse alla rete, pur essendo di per sé una *sicurezza logica*, impedendone il raggiungimento ai dispositivi non autorizzati.

Funziona sia su connessioni wired che wireless, anche se viene raramente supportato ed utilizzato nelle connessioni cablate in quanto, spesso, una protezione fisica perimetrale viene considerata sufficiente.

Il 802.1X determina unicamente la procedura di autenticazione che deve essere svolta, mentre la definizione degli standard dei messaggi e del trasporto viene definita da altri standard, ad esempio EAP per il contenuto dei messaggi ed EAPOL e RADIUS per il loro trasporto.

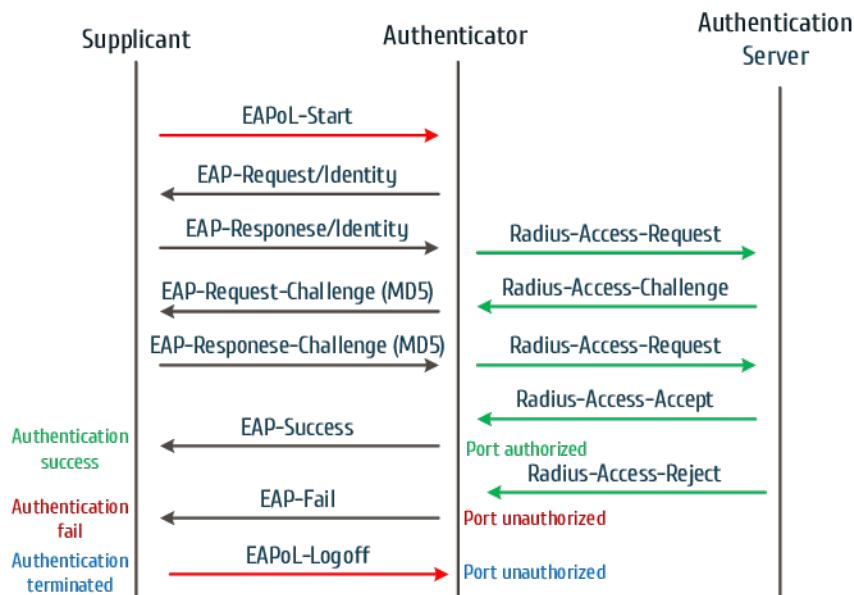


Figura 5.4: Procedura di autenticazione 802.1X

5.2.2 Extensible Authentication Protocol

Il Extensible Authentication Protocol, usualmente chiamato semplicemente EAP, è un framework di autenticazione che definisce la struttura dei messaggi.

Lo standard include svariate tipologie di messaggio, in modo tale da poter fornire molteplici metodologie di login, come ad esempio combinazioni username e password, utilizzo di certificati o mediante un segreto condiviso.

Non essendo un protocollo di rete ha la necessità di essere incapsulato in un messaggio per poter essere inviato, ad esempio all'interno del protocollo *RADIUS_G* oppure nel protocollo di rete dedicato *EAPoL_G*.

5.2.3 Windows Network Policy Server

Network Policy Server, spesso abbreviato in NPS, in italiano "Server dei criteri di rete", è una tecnologia per il controllo dell'accesso alla rete.

Decreta chi può accedere alla rete ponendo delle restrizioni ed utilizzare il protocollo $RADIUS_G$ per comunicare.

Un server che lo implementa può decretare indipendentemente l'accesso o meno dei vari dispositivi, costituendo quindi un RADIUS server, oppure può inoltrare la richiesta ad un altro server NPS, quindi coprendo il ruolo di RADIUS proxy.

5.2.4 Active Directory

Active Directory è un insieme di servizi di rete adottati dai sistemi operativi Microsoft.

Sono gestiti da un $Domain Controller_G$ e definisce le modalità di accesso alle risorse da parte degli utenti.

Le risorse possono essere account utente, account relativi a un computer, cartelle condivise, stampanti e servizi di varia natura. I privilegi di accesso alle varie risorse sono determinati mediante dei criteri di gruppo.

5.2.5 CAPsMAN

CAPsMAN, per esteso Controlled Access Point system MANager, traducibile in "sistema di gestione di access point controllati", è una funzionalità per la gestione degli accessi fornita da MikroTik assieme ai suoi access point.

La sua funzionalità principale è la propagazione di una configurazione comune per l'accesso Wireless a tutti gli apparati presenti nella rete.

Consente l'identificazione dei client che si connettono mediante un server RADIUS e permette anche di reindirizzare dinamicamente gli utenti su VLAN diverse.

Risulta molto utile in caso di estensione della rete, in quanto riduce notevolmente la configurazione iniziale di ogni access point, diminuendo a sua volta il rischio di commettere errori di configurazione.

5.3 Strumenti di lavoro

5.3.1 Microsoft Visio

Microsoft Visio è uno strumento dedito alla creazione di grafici ed organigrammi. Nell'abito dello stage si è rivelato utile per la creazione della mappa della rete, in quanto facilmente utilizzabile e gestibile anche da persone senza una elevata conoscenza dell'informatica o di linguaggi dediti allo scopo.

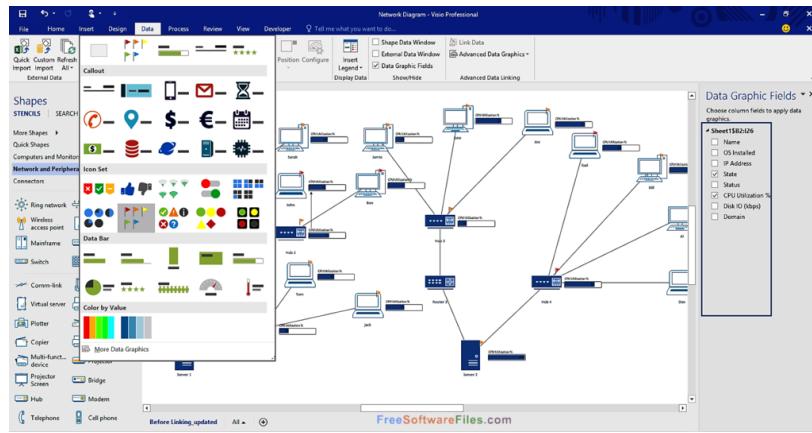


Figura 5.5: Interfaccia di Visio

5.3.2 OpenOffice Calc

OpenOffice Calc è un software per la gestione di fogli elettronici, che consente anche di aprire i formati gestiti da LibreOffice Calc e Microsoft Excel.

È stato impiegato per la realizzazione della lista dei dispositivi, in quanto consente una consultazione veloce e l'esportazione in svariati formati.

	A	B	C	D	E	F	G	H	I	J
1	Country	Population (per 1k)	Downloads Wikipedia	Internet Users per 1k	AOO per 1K population	Rank (AOO per internet users)	(AOO per Population) Users			
188	San Marino	1.067	32.457	15.781	32.874	68	13	4		
189	Netherlands	568.068	16.751.323	15.371.200	39.912	37	12	14		
190	Malta	100	53.333	3.908	30.017	34	11	18		
191	Finland	212.062	5.387.000	4.700.192	48.362	45	10	10		
192	Switzerland	333.002	8.000.000	6.688.285	41.626	50	9	9		
193	Estonia	56.256	1.294.000	981.467	42.701	56	8	7		
194	Germany	3.602.587	81.799.900	67.621.622	44.042	53	7	8		
195	Belgium	529.150	11.041.266	8.136.552	47.925	65	6	6		
196	Ukraine	224.151	4.570.610	13.811.224	49.042	16	5	44		
197	Italy	3.160.660	60.813.306	34.657.545	51.973	91	4	2		
198	Luxembourg	29.768	517.000	457.451	57.617	65	3	5		
199	Monaco	2.346	35.000	22.940	67.086	102	2	1		
Sum		1.041.020	1.041.020	1.041.020	1.041.020	1.041.020	1.041.020	1.041.020	1.041.020	1.041.020

Figura 5.6: Interfaccia di Calc

5.3.3 GreaseMonkey

GreaseMonkey è un plugin disponibile per il browser Mozilla Firefox che consente l'esecuzione di script in linguaggio JavaScript.

Permette anche lo store di variabili, il caricamento di librerie esterne e l'esecuzione con permessi privilegiati.

È stato utilizzato durante le attività di stage per automatizzare operazioni ripetitive, consentendo di avere più tempo libero da dedicare ad altre attività.



Figura 5.7: Logo di GreaseMonkey

5.3.4 Putty

Putty è un client SSH, Telnet e seriale combinato con un emulatore di terminale per consentire una iterazione con dispositivi remoti.

È stato ampiamente utilizzato per le connessioni SSH e seriale per la configurazione e il controllo dei dispositivi di rete.

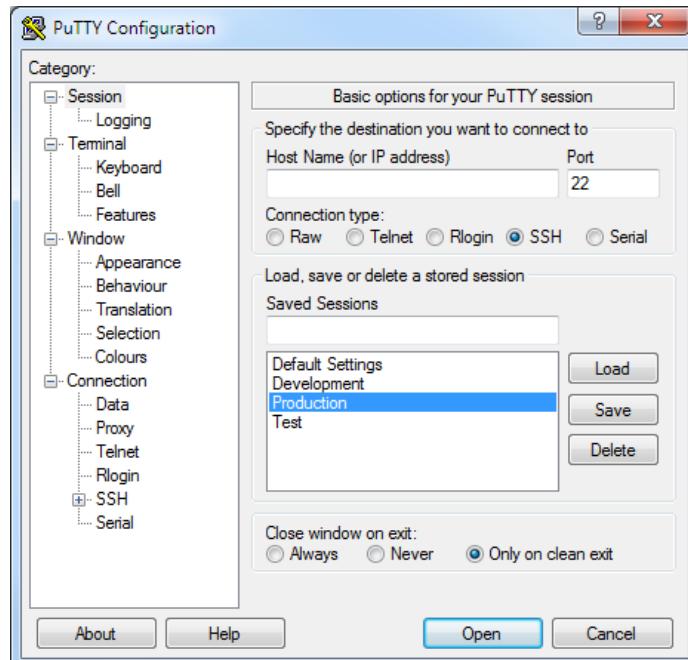


Figura 5.8: Schermata iniziale di Putty

5.3.5 Microsoft Telnet

Il client Telnet fornito assieme al sistema operativo Microsoft Windows permette di collegarsi a dispositivi remoti tramite protocollo Telnet mediante un qualsiasi terminale.

È stato preferito a Putty per il fatto che risulta più veloce ed immediato da utilizzare, in quanto accessibile direttamente dalla console del sistema.

5.3.6 MySQL Command-Line Tool

La shell MySQL è in interfacciamento a linea testuale al database MySQL, che permette una iterazione con la struttura ed i dati in esso contenuto.

Nell'ambito del progetto è stato impiegato principalmente in concomitanza con rConfig, in quanto l'incompletezza del programma ha richiesto svariate volte una modifica manuale alla base di dati dalla quale attingeva le informazioni.

5.3.7 Notepad++

Notepad++ è un editor di file testuali disponibile per sistemi operativi Microsoft Windows.

La sua utilità nell'ambito del progetto è stata l'esecuzione di espressioni regolari per permettere una rapida conversione del formato dei dati, consentendo di convertire file CSV in matrici JavaScript.

È stato favorito rispetto ad altri editor in quanto possedevo già dimestichezza con esso.

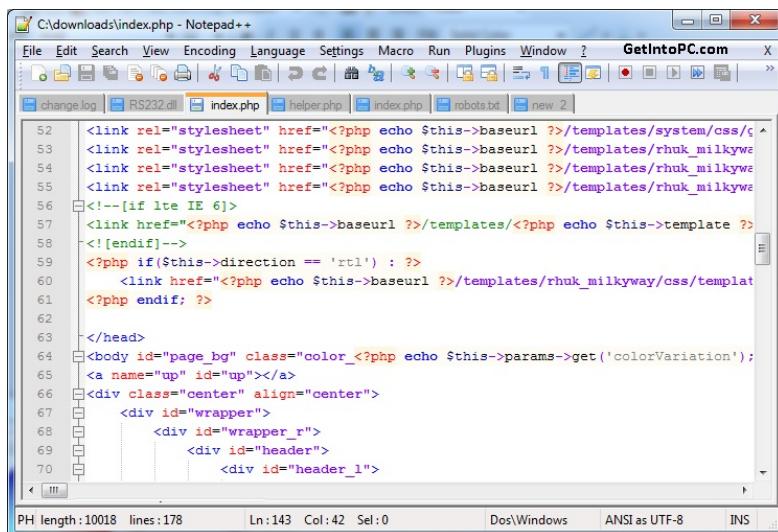


Figura 5.9: Interfaccia di Notepad++

5.3.8 Vim

Vim è un editor di file testuali disponibili su molteplici piattaforme, di storica rilevanza nel mondo Unix.

Essendo spesso preinstallato, disponibile per un numero elevato di sistemi ed eseguibile da terminale si è rivelato comodo per la modifica dei file di configurazione sulle macchine virtuali, grazie anche alle sue modalità di iterazione con il testo.

Figura 5.10: Interfaccia di Vim

5.3.9 FileZilla

FileZilla Client è un software che permette il trasferimento di file in Rete attraverso il protocollo FTP.

Si è rilevato utile per la gestione dei file sulle macchine virtuali e sui dispositivi MikroTik, permettendo un facile trasferimento delle configurazioni e delle pagine web che si sono utilizzate durante tutto lo stage.



Figura 5.11: Logo di FileZilla

Capitolo 6

Realizzazione

6.1 Analisi

- **Periodo previsto:** dal 04/06/2018 al 08/06/2018;
- **Numero di ore previste:** 40h;
- **Periodo effettivo:** dal 04/06/2018 al 08/06/2018;
- **Numero di ore effettive:** 40h.

Una delle prime attività svolte è stata la raccolta della documentazione preesistente e la sua analisi.

Sono subito emerse svariate incongruenze tra i vari documenti in quanto alcuni erano datati, per questo motivo si è dovuto confrontarli, individuare l'informazione corretta ed aggiornare gli altri.

Non si sono però avuti scostamenti di tempo in quanto la documentazione era in considerevole quantità.

6.1.1 Lista apparati

Come base di questa attività si sono utilizzati alcuni documenti Excel che riportano informazioni parziali che sono state integrate tra loro. Da questa attività è emerso che c'erano informazioni assenti per alcuni devices, che sono state recuperate e documentate.

Successivamente si è andato ad aggiungere la posizione GPS di ogni dispositivo, utilizzando i dati presenti nel software di monitoraggio PRTG e individuando, con l'aiuto di Google Maps, le coordinate mancanti.

I dispositivi possedevano già dei nominativi che ne indicavano la locazione all'interno del contesto, che sono stati mantenuti.

6.1.2 Analisi sistemi di sicurezza fisica

La sicurezza fisica era perseguita prevalentemente controllando l'accesso fisico ai dispositivi di rete. Gli switch sono chiusi a chiave negli appositi armadi e, ove possibile, mantenuti all'interno di strutture dove l'accesso è consentito solo al personale dedicato.

Era già presente una suddivisione in VLAN attua a impedire l'accesso alle risorse a coloro che non ne possiedono i permessi, ma da sola non era sufficiente a garantire la sicurezza.

Un possibile attacco è forzare un armadietto di rete ed utilizzare una porta Ethernet untagged per poter connettersi ai dispositivi di quella VLAN. Questo risulta molto pericoloso considerando che la VLAN di manutenzione, presente in quasi tutti gli switch, permette l'accesso a tutti gli altri apparati di rete.

Analogo discorso per le reti WiFi dedicate al personale, nel quali spesso si connettono dispositivi personali o si forniscono le chiavi di autenticazioni ad amici e parenti, mettendo a rischio le risorse raggiungibili.

In questo contesto si è andati ad operare sul controllo d'accesso sulle reti wireless, impedendo ad un dispositivo non riconosciuto di entrare in una VLAN semplicemente connettendosi ad una rete, ma richiedendogli informazioni aggiuntive e certificate mediante lo standard 802.1X.

Una possibile estensione dell'attività di stage potrebbe essere ampliare l'utilizzo del protocollo 802.1X anche sulla parte cablata della rete, al fine di inserire una ulteriore protezione.

6.1.3 Analisi sistemi di monitoraggio

La rete analizzata presentava già un software per il monitoraggio, denominato PRTG Network Monitor.

Il suo compito era quello di controllare che tutti i sensori in esso inseriti appartenenti ai devices funzionassero correttamente, avvisando qualora ci fossero dei problemi.

Una delle problematiche fondamentali di questo software era la difficoltà nel tracciare grafici relativi alla connessione e alla qualità del servizio, impedendo di identificare eventuali colli di bottiglia, pacchetti persi o errori di trasmissione.

Questo software veniva utilizzato in versione gratuita e quindi presentava alcune limitazioni, la più problematica è la quantità di sensori che può monitorare, limitata a 1000, che non consentiva di controllare in modo soddisfacente tutti gli apparati di rete presenti.

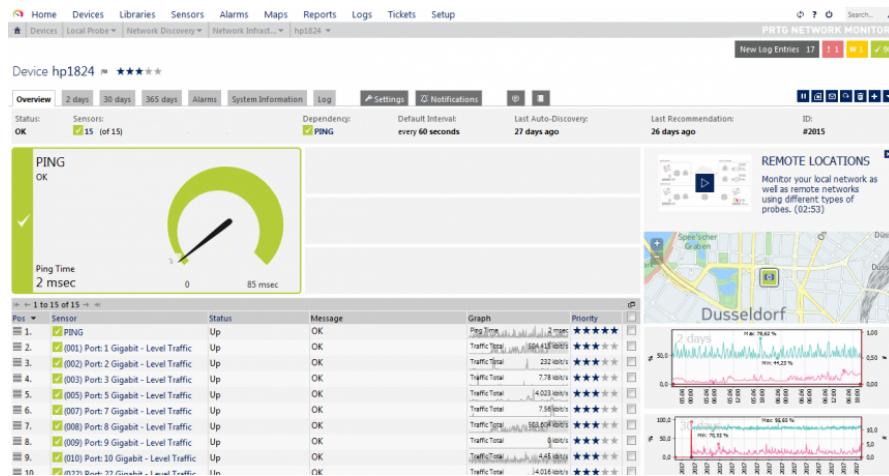


Figura 6.1: Schermata di PRTG Network Monitor

6.1.4 Schema di rete

Per facilitare tutte le attività successive di configurazione e monitoraggio si è proceduto alla redazione di uno schema di rete.

Essendo già disponibile uno schema datato 2015 della rete realizzato dal cliente in Microsoft Visio si è scelto di procedere con lo stesso software.

A supporto di questo lavoro si sono utilizzate svariate mappe prodotte in tem-

pi e per fini diversi tra di loro, la cui integrazione ha evidenziato degli errori che sono stati segnalati.

La posizione degli apparati è stata modificata in modo da seguire più fedelmente la loro collocazione reale, favorendone una identificazione più veloce.

Lo schema di rete di partenza e quello realizzato, presentanti il nome, il modello di dispositivo e l'indirizzo ip, sono presenti in Appendice A.

Si può notare come nella prima versione c'erano molte incongruenze nella forma nella quale sono stati riportati i dati, in quanto è stata prevalentemente scritta ed utilizzata da una singola persona e quindi non c'è stata attenzione rivolta alla chiarezza espositiva.

Alcune informazioni riportate sugli schemi sono state alterate o omesse per motivi di sicurezza e di privacy.

6.2 Progettazione

- **Periodo previsto:** dal 11/06/2018 al 22/06/2018;
- **Numero di ore previste:** 80h;
- **Periodo effettivo:** dal 11/06/2018 al 26/06/2018;
- **Numero di ore effettive:** 96h.

Una volta terminata la fase di analisi della rete si è proceduto a progettare tutti i software e le configurazioni che saranno implementate.

Lo svolgimento di questa attività ha occupato una durata temporale maggiore di quella prevista, in quanto è stato necessario avere un dialogo con il cliente per meglio capire le sue necessità e si è dovuto individuare e studiare le tecnologie da utilizzare.

6.2.1 Progettazione Observium

Prima di installare e mettere in funzione il software di monitoraggio Observium lo si è provato localmente, al fine di individuare pregi e difetti del programma e comprendere quindi il miglior modo di utilizzarlo.

Inizialmente è stato istanziato inserendo al suo interno 5 apparati di rete, sui quali si sono testate svariate configurazioni per comprendere gli aspetti che potessero ritornare utili al monitoraggio della rete e quelli che, invece, non erano efficaci per il contesto.

Si è notato che la posizione GPS rilevata automaticamente del software era troppo imprecisa, ma la funzionalità è di elevata importanza visto l'estensione della rete. Si è dunque deciso di inserirle manualmente, sovrascrivendo il dato presente.

Un'altra opzione che si è rilevata fondamentale è la disabilitazione delle interfacce non in uso, che avrebbero generato avvertimenti inutili.



Figura 6.2: Interfacce visualizzate all'interno di Observium

Ulteriormente il software visualizzava anche l'area di appartenenza dei devices prelevandola dalla loro configurazione, ma risultava poco indicativa, quindi si è scelto di sovrascriverla indicando la locazione con più precisione.

6.2.2 Progettazione rConfig

Analogamente a quanto effettuato con Observium, anche per rConfig si è eseguito un test per comprenderne le potenzialità e la migliore modalità di utilizzo. Sono stati inseriti anche per esso 6 dispositivi, in modo tale da avere almeno un dispositivo per ogni modello di apparato in utilizzo.

Si sono notati da subito alcuni problemi, sia di utilizzo che di sicurezza, e di conseguenza si è dovuto fare particolare attenzione nella progettazione, in modo da impedire malfunzionamenti ed accessi non autorizzati.

Uno dei problemi di sicurezza riscontrati, che si è scoperto essere presente anche nelle altre istanze utilizzate dall'azienda, è una vulnerabilità *SQL injection* che permetteva di ottenere una lista completa dei report effettuati, compresi quelli rimossi o non accessibili per l'account in uso.

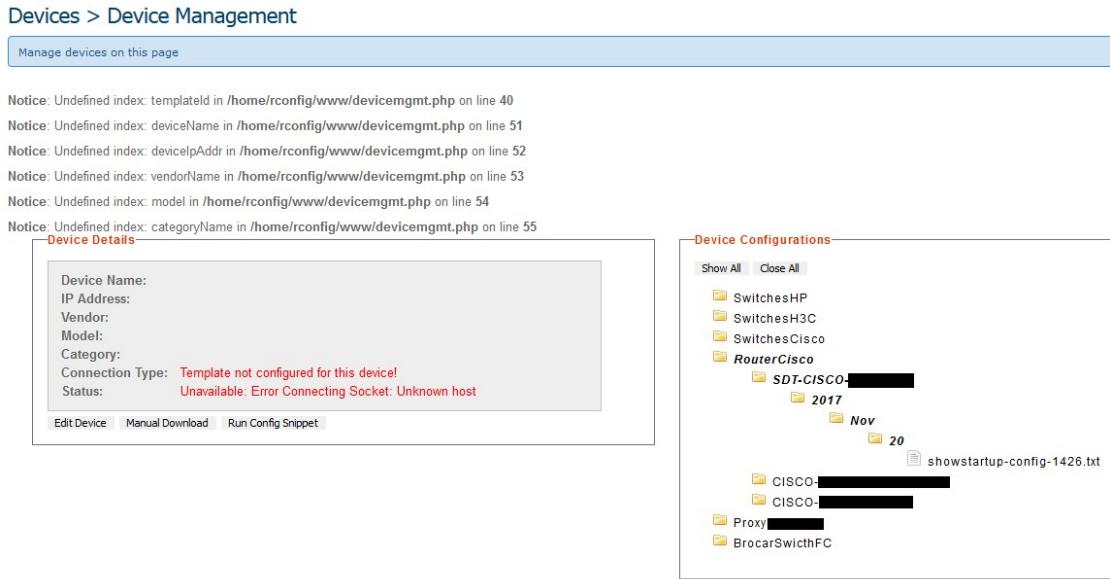


Figura 6.3: Attacco SQL injection su rConfig, sulla destra tutte le configurazioni navigabili

6.2.3 Progettazione della rete WiFi dedita agli uffici

Per permettere una estensibilità della rete senza l'intervento di un tecnico per la sua configurazione si è scelto di utilizzare CAPsMAN.

La struttura della tecnologia CAPsMAN si basa su un router centrale, prodotto da MikroTik, che gestisce e fornisce le configurazioni. Su questo router vengono collegati, mediante la VLAN a lui dedicata, gli Access Point, che provvederanno autonomamente a recuperare ed applicare le impostazioni corrette.

Questa metodologia permette, in caso di estensione della rete, di evitare una configurazione manuale dei dispositivi, che potrebbe presentare errori di distrazione e compromettere la sicurezza.

Un'altra caratteristica di estrema importanza è che le impostazioni, essendo centralizzate, possono essere modificate unicamente nel router e le modifiche vengono poi trasmesse automaticamente a tutti i dispositivi.

Il sistema così organizzato però introduce un potenziale pericolo, in quanto il router che gestisce CAPsMAN è unico e rappresenta un single point of failure.

Politiche di sicurezza

Durante la progettazione si è decretato anche il numero di SSID wireless da impiegare e le loro modalità di accesso.

L'attenzione è stata posta sulle reti utilizzate dal personale, in quanto consentono l'accesso a risorse di elevata importanza e per tale ragione devono essere protette. Per tali motivazioni si è scelto di creare 3 reti wireless, così definite:

- **Corporate:** rete dedita alla connessione dei computer dediti ad attività lavorative, consente l'accesso alle risorse;
- **Mobile:** rete dedicata ai dispositivi personali e/o lavorativi dei dipendenti, come smartphone e tablet, che non richiedono l'accesso a risorse;
- **Guest:** rete atta a fornire una connettività internet agli ospiti degli uffici.

Le misure di autenticazioni sono le seguenti:

- **Corporate:** l'accesso è consentito previa autenticazione mediante EAP utilizzando le proprie credenziali Active Directory e usufruendo del relativo certificato digitale;
- **Mobile:** l'accesso è consentito previa autenticazione mediante EAP utilizzando le proprie credenziali Active Directory, senza la necessità di usufruire di un certificato digitale;
- **Guest:** l'accesso è consentito mediante l'inserimento di una password di bassa complessità e la registrazione su un *captive portal*_G.

Per l'attualizzazione di tali politiche non sarà sufficiente utilizzare il router MikroTik per determinare l'accettazione o il rifiuto delle richieste di autenticazione, ma saranno necessari dei servizi esterni, che verranno contattati mediante RADIUS.

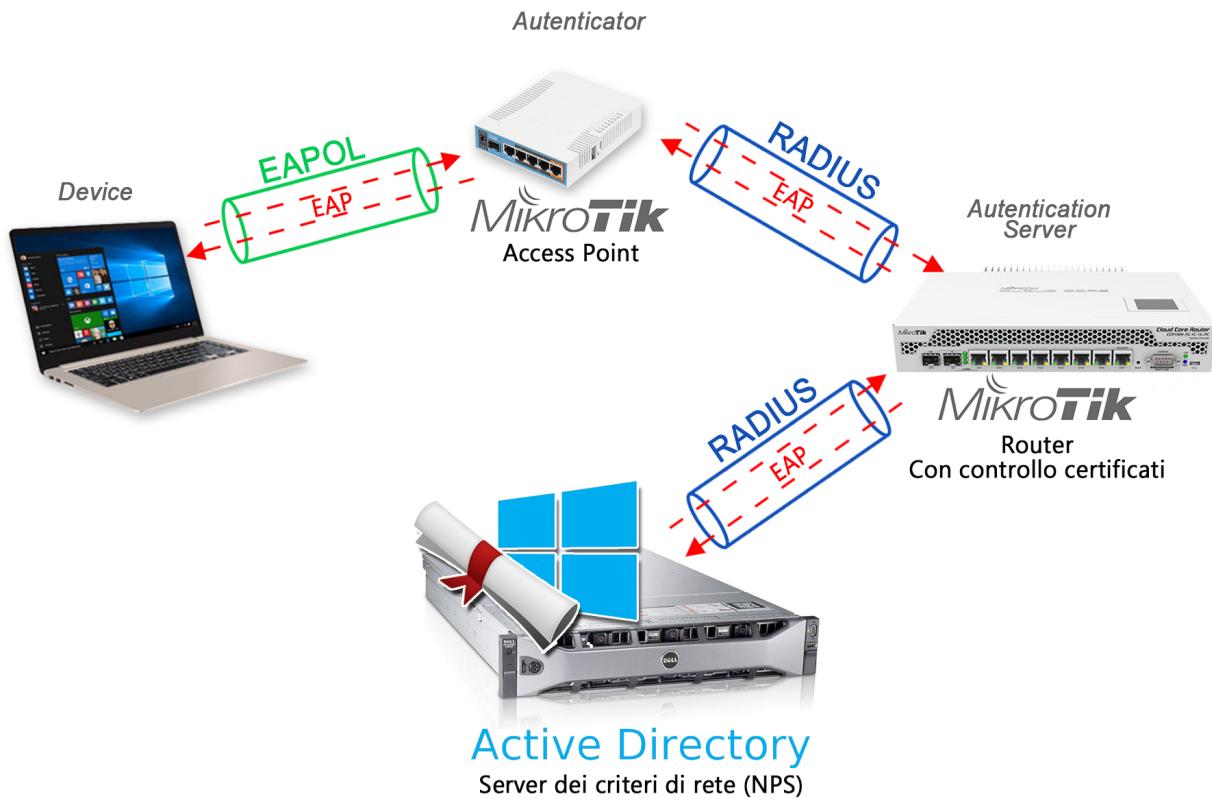


Figura 6.4: Schema dei dispositivi e dei protocolli usati per le reti Corporate e Mobile

Per quanto riguarda la rete Corporate il Auntenticator, non contenendo nessuna politica per l'approvazione delle richieste, si comporterà da Proxy ed invierà la richiesta al server NPS.

Il servizio Microsoft verificherà innanzitutto che il certificato digitale fornito venga utilizzato, rifiutando immediatamente la richiesta nel caso fosse non crittografata o non conforme a quanto atteso. Invece, se il certificato è stato correttamente utilizzato, procederà a effettuare un riscontro tra le credenziali e gli account presenti nell'Active Directory, individuando la presenza o meno dell'utente.

Nel caso la richiesta provenisse dalla rete Mobile la procedura risulta la medesima, con l'eccezione che il certificato non viene richiesto.

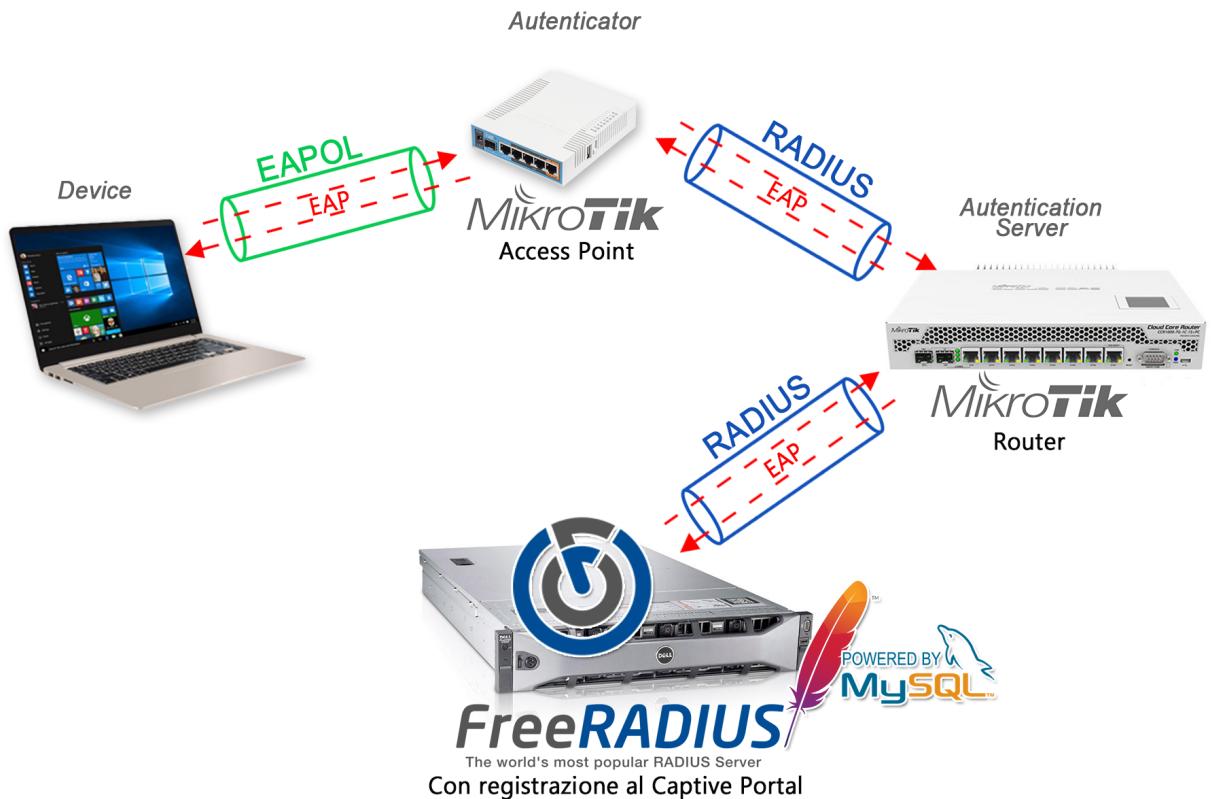


Figura 6.5: Schema dei dispositivi e dei protocolli usati per la rete Guest

Infine, per la rete Guest, ci sarà la necessità di avere un servizio RADIUS esterno al router al quale effettuare le richieste, in modo tale che sia sicuro, facilmente raggiungibile e mantenibile mediante una interfaccia web.

Sullo stesso server, per motivi di sicurezza, sarà presente anche parte del Captive Portal, realizzato con i servizi Apache HTTP e MySQL.

6.2.4 Progettazione Captive portal

Per la progettazione del *captive portal*_G si è scelto di utilizzare come modello uno già in uso in alcune soluzioni sviluppate da Wintech, in modo tale da dedicare meno tempo alla progettazione e porre l'attenzione sugli aspetti di networking e di sicurezza.

La schermata di login si presenta con alcune form dedito all'inserimento della propria e-mail, della selezione di uno sponsor e della durata dell'account. Gli sponsor avranno il compito di confermare o rifiutare la richiesta e potranno essere gestiti dall'amministratore nella apposita area di amministrazione.

Figura 6.6: Schermata per la richiesta di un account

Una volta effettuata la richiesta di registrazione verrà inviata una e-mail allo sponsor, ed in caso di approvazione verrà comunicata la password di accesso al richiedente.

L'account avrà una durata temporale limitata, scelta dall'utente tra serie di opzioni decretate dall'amministratore. Questa caratteristica serve per scoraggiare eventuali dipendenti a farne uso per le loro attività lavorative e per impedire un accumularsi di vecchi account registrati ma non più utilizzati.

La rete presenta anche una password di accesso, di bassa complessità, in modo tale da evitare un possibile spam, o flooding, di e-mail ai danni degli sponsor.

Si è scelto di mantenere la procedura di login all'interno del router MikroTik per evitare redirezioni inutili, il quale andrà a controllare la validità dell'account comunicando con il protocollo RADIUS verso i relativi servizi.

La registrazione e la parte di amministrazione avverranno in autonomia su una macchina virtuale, che avrà il compito di far interagire l'interfaccia web con il database in modo tale da aggiornare le informazioni contenute nel RADIUS e di comunicare le credenziali tramite e-mail.

Il dispositivo MikroTik presenta un Captive Portal di default, che sarà quindi personalizzato modificandone le grafica ed inserendo tutti i collegamenti verso le pagine di registrazione ed amministrazione presenti sulla macchina virtuale.

Di seguito sono riportate alcune diagrammi per meglio comprendere l'iterazione delle varie parti tra di loro.

Per semplificare lo schema è stato omesso l'Autenticator, cioè l'Access Point, in quanto la sua iterazione avviene su un livello inferiore rispetto a quello analizzato attualmente.

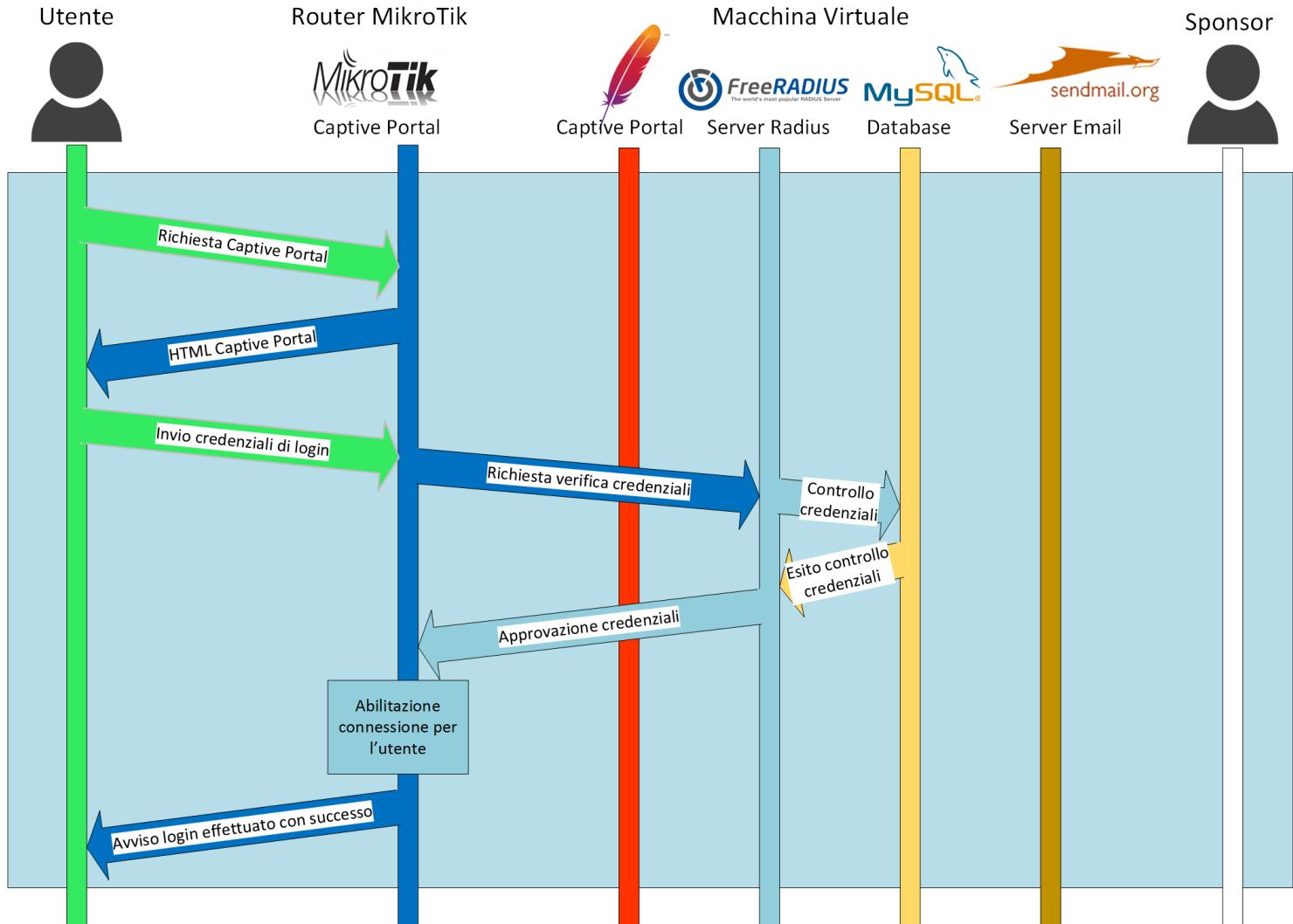


Figura 6.7: Sequenza per effettuare il login

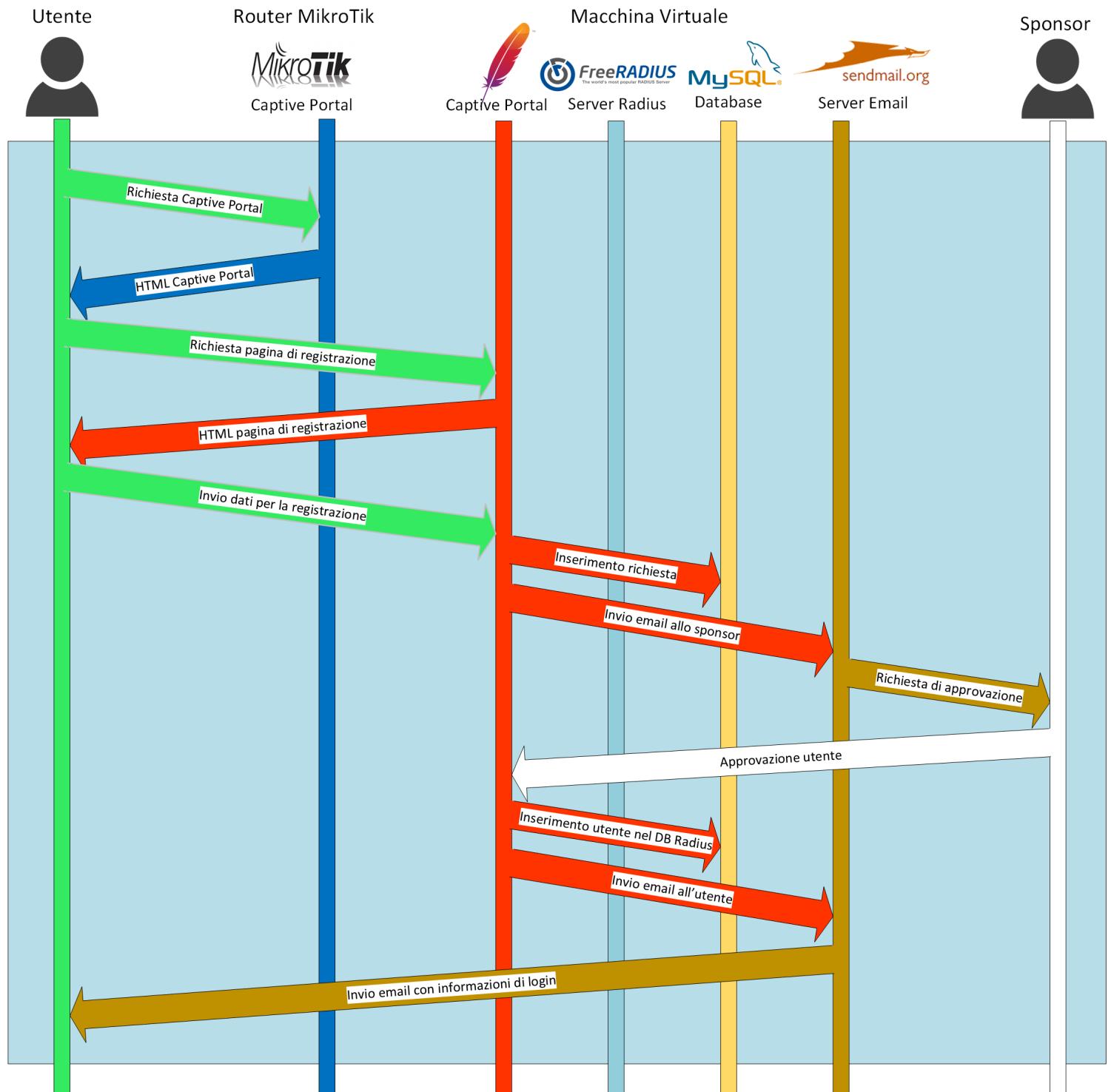


Figura 6.8: Sequenza per effettuare la registrazione

6.2.5 Progettazione entry DNS

Definizione name-convention

La name-convention scelta per la denominazione degli apparati è la seguente:

DEVICE-ZONA [-LOCAZIONE] [-NUMERO_INC]

Nella quale i campi presenti indicano:

- **DEVICE**: Il modello del dispositivo installato, ad esempio "HP-2520-8-PoE";
- **ZONA**: La zona di appartenenza del dispositivo, ad esempio "ZONA-A", "EDIFICI" o "AMMINISTRAZIONE";
- **LOCAZIONE**: La locazione geografica utilizzata per identificare il dispositivo, opzionale nel caso basti la zona per l'identificazione univoca dell'armadio;
- **NUMERO_INC**: Numero incrementale, da utilizzare nel caso siano presenti più apparati nello stesso armadio di rete.

Questa convenzione è stata scelta in accordo con il cliente per permettere una identificazione veloce dell'apparato di rete anche ai manutentori, in linea con le denominazioni utilizzate internamente.

La presenza del modello di dispositivo è contrario alla best-practice da seguire, in quanto la sostituzione di un apparato con un modello successivo richiede la sostituzione della voce all'interno del DNS e di conseguenza la riconfigurazione dei software di monitoraggio. Ciò è stato richiesto in quanto si favorisce l'immediatezza dell'identificazione del dispositivo a discapito della manutenibilità, tenendo in considerazione che gli upgrade non sono frequenti.

Definizione nomi DNS per gli apparati

Dopo aver definito la name-convention da utilizzare ed avere avuto l'approvazione dal cliente si è proseguito applicandola a tutti gli apparati.

È quindi stato individuato il nome DNS per ogni dispositivo ed è stato riportato all'interno del documento contenente la lista degli apparati.

6.2.6 Produzione della prima bozza della documentazione progettuale

Durante questo periodo è stata scritta la prima bozza della documentazione. Si è proceduto ad inserire al suo interno la lista degli apparati, lo schema della rete e tutte le informazioni utilizzate durante queste prime settimane.

6.3 Implementazione

- **Periodo previsto:** dal 25/06/2018 al 06/07/2018;
- **Numero di ore previste:** 80h;
- **Periodo effettivo:** dal 27/06/2018 al 11/07/2018;
- **Numero di ore effettive:** 88h.

L'implementazione di quanto progettato ha richiesto un numero di ore maggiore di quanto preventivato a causa delle problematiche sorte dall'utilizzo di rConfig. Una parte di queste ora aggiuntive sono però state ammortizzate dal risparmio di tempo avuto nella fase di data-entry relativa ai dispositivi, in quanto è stato ampliamene velocizzato dall'utilizzo di scripting.

6.3.1 Preparazione dell'ambiente

Inserimento dei dispositivi sul DNS interno

Per consentire una adeguata implementazione di Observium e rConfig era richiesto l'utilizzo dei nomi DNS degli apparati e non dell'indirizzo IP.

Si è dunque proceduto a comunicare la lista dei nomi e dei relativi IP dei dispositivi al responsabile affinché vengano inseriti nel sistema, in quanto non c'era la disponibilità di accedere direttamente alle impostazioni del DNS.

Implementazione Virtual Machine

Per consentire l'esecuzione continua dei software sono state create due Virtual Machine, o macchine virtuali.

Il server utilizzato per tale fine è quello del cliente, utilizzante le tecnologie prodotte da VMware per la virtualizzazione.

Le due macchine virtuali sono state entrambe create con CentOS Linux, in quanto gratuito e già conosciuto nel contesto aziendale.

Creazione laboratorio per le nuove politiche

Prima di procedere alla produzione si sono testate le configurazioni in un laboratorio.

Per tale fine sono stati utilizzati uno switch HP 2530-8G PoE+ e svariati Access Point MikroTik cAP ac RBcAPGi-5acD2nD, collegati a un controller MikroTik CCR1009-7G-1C-1S+.



Figura 6.9: Switch HP 2530-8G PoE+



Figura 6.10: Access Point MikroTik cAP ac



Figura 6.11: Controller MikroTik

6.3.2 Configurazione del monitoraggio con Observium

Analogamente con quanto effettuato con RConfig è stato effettuato l'inserimento di tutti i dispositivi e alla loro configurazione in Observium.

Questa operazione è stata più complessa rispetto all'altro software, in quanto richiedeva una aggiunta iniziale di ogni dispositivo, seguito dall'attesa della sua identificazioni per poi terminare con l'aggiunta delle informazioni aggiuntive. Seguendo quanto deciso nella fase di progettazione si è andato ad inserire, sempre mediante l'aiuto di GreaseMonkey, la sua locazione e le sue coordinate GPS.

Per completare l'attività si è anche dovuto segnalare al software tutte le interfacce non utilizzate, in modo tale che non venissero generati avvisi a causa della

loro inoperatività.

Al termine dell'operazione gli elementi inseriti all'interno del software erano i seguenti:

- 94 apparati di rete;
- 7 apparati wireless;
- 3064 interfacce;
- 452 sensori;
- 272 periferiche.

I sensori presenti sono principalmente relativi all'alimentazione ed in alcuni casi alla temperatura del dispositivo, mentre i componenti aggiuntivi sono ventole di raffreddamento ed alimentazione.

Questi numeri dimostrano l'impossibilità di mantenere un controllo soddisfacente della rete utilizzando la versione gratuita di PRTG Netwrk Monitor, che consentiva in totale il monitoraggio di 1000 elementi.

6.3.3 Configurazione del versioning con RConfig

Per la configurazione di rConfig si è proceduto ad automatizzare l'inserimento dei dati, che altrimenti avrebbe consumato una ingente quantità di tempo visto il numero di dispositivi presenti.

Come base di riferimento per l'inserimento dei dati si è attinto dalla tabella dei dispositivi precedentemente realizzata, che è stata esportata in formato csv_G . Successivamente si è modificato il formato dei dati esportati, operando per mezzo di una *espressione regolare_G*, al fine di convertirlo in una matrice in linguaggio JavaScript per il suo utilizzo all'interno del browser.

Si è quindi sviluppato uno script JavaScript, visionabile in Appendice B, che mediante il plug-in GreaseMonkey consentiva il caricamento automatico dei dati precedentemente posti in forma corretta.

Per terminare è stato eseguito lo script, che ha proceduto all'inserimento degli apparati.

Scheduling backup delle impostazioni con rConfig

Per completare la messa in funzione di rConfig si sono suddivisi i dispositivi in gruppi secondo la loro locazione ed si sono predisposti dei backup periodici.

Per non sovraccaricare la rete si è scelto di svolgere il backup a cadenza settimanale durante la notte, facendo attenzione a non sovrapporsi al backup giornaliero degli altri apparati. Gli orari sono stati scelti in modo tale che i task non si sovrappongano tra di loro, così da evitare eventuali problemi.

Questa attività si è rilevata più ostica del previsto a causa di molte problematiche di rConfig, rimaste per ora irrisolte anche nella versione più recente.

Inizialmente si sono notati un numero di backup superiori a quanto schedulato. Questo avveniva perché le attività inserite e poi rimosse non risultavano più presenti dall’interfaccia web, ma rimanevano in esecuzione. Per arginare questo problema si è dovuto accedere direttamente al database dell’applicazione mediante MySql e correggere le informazioni in esso contenute.

Durante la correzione del problema precedente si sono rilevate altre anomalie all’interno del database, soprattutto dovute a una scarsa normalizzazione dei dati e a una strutturazione non adatta ad un database di tipo SQL. Pertanto si è dovuto controllare eventuali incongruenze e correggerle, in modo da evitare comportamenti inaspettati in futuro.

Nell’immagine seguente si può notare un esempio di quanto affermato. I dispositivi, chiamati nodi, non hanno una relazione molti a molti con i task, ma bensì contengono delle colonne con il nome riferito all’id del tast, il cui valore è un enumeratore che ne indica l’abilitazione.

rConfig nodes	
id : int(10)	
taskId556251 : varchar(20)	
taskId450655 : varchar(20)	
taskId637140 : varchar(20)	
taskId842385 : varchar(20)	
taskId164891 : varchar(20)	
taskId687418 : varchar(20)	
taskId669000 : varchar(20)	
deviceName : varchar(255)	
deviceUsername : varchar(255)	
devicePassword : varchar(255)	
deviceEnablePassword : varchar(255)	
deviceIpAddr : varchar(255)	
devicePrompt : varchar(255)	
deviceEnablePrompt : varchar(255)	
# nodeCatId : int(10)	
# templateId : int(10)	
vendorId : varchar(255)	
model : varchar(255)	
nodeVersion : varchar(255)	
nodeAddedBy : varchar(255)	
# defaultCreds : int(1)	
defaultUsername : varchar(255)	
defaultPassword : varchar(255)	
defaultEnablePassword : varchar(255)	
deviceDateAdded : date	
deviceLastUpdated : date	
# status : int(10)	
custom_Location : varchar(255)	

rConfig tasks	
id : int(6)	
# taskType : int(3)	
taskname : varchar(255)	
taskDescription : varchar(255)	
# snipld : int(10)	
crontime : varchar(255)	
croncmd : varchar(255)	
addedBy : varchar(255)	
dateAdded : date	
catId : varchar(255)	
catCommand : varchar(255)	
# status : int(2)	
# mailConnectionReport : int(10)	
# mailErrorsOnly : int(10)	
# complianceId : int(10)	

Figura 6.12: Esempio della scarsa normalizzazione dei dati in rConfig

Backup configurazioni MikroTik

Una volta avuto a disposizione i device MikroTik è emerso un problema inaspettato con rConfig, che non riusciva a completare il backup delle configurazioni su tali dispositivi.

Il problema era causato da una serie di caratteri non stampati a schermo utilizzati dai dispositivi, che rConfig non sapeva rilevare correttamente, impedendogli di compiere i passaggi di login necessari.

Per risolvere tale problema in modo veloce, efficiente e duraturo nel tempo si è scelto di incaricare il dispositivo stesso dell'effettuazione del backup. Per raggiungere tale scopo è stato creato uno script, visibile in Appendice C, che permette il salvataggio automatico delle proprie configurazioni su un server FTP.

Una volta verificato il corretto funzionamento dello script è stato schedulato in modo tale avvenga automaticamente ad intervalli prefissati.

Ulteriormente il server FTP è stato dotato di un demone HTTP Apache, in modo

da consentire la navigazione dei backup effettuati. Per migliorare la fruizione del sito si è utilizzato Directory Lister, il quale è stato modificato per richiedere l'inserimento di una password.

File	Size	Last Modified
AP01	-	2018-07-11 13:04:03
AP02	-	2018-07-11 10:22:51
AP03	-	2018-07-11 10:22:51
AP04	-	2018-07-11 10:22:51
AP05	-	2018-07-11 10:22:51
AP06	-	2018-07-11 10:22:51
Router	-	2018-07-11 10:48:39

Powered by, [Directory Lister](#)

Figura 6.13: Lista delle cartelle con i backup in Directory Lister

6.3.4 Configurazione nuovi apparati di rete

Per il collegamento tra gli access point e il router si è andati ad utilizzare una VLAN ad essi dedicata.

Sopra di essa è stato creato un datapath costituito da un bridge che consenta la comunicazione dei dispositivi connessi alle reti wifi.

Per motivi di sicurezza si è scelto di creare tre tunnel Ethernet over IP (EoIP) per incanalare i tre flussi di dati provenienti dai tre SSID wifi.

Così facendo si è ottenuta una elevata sicurezza, unita alla facilità di installazione di un nuovo dispositivo, in quanto è necessario solamente trasportargli la VLAN che utilizza, nell'immagine sottostante denominata "VLAN AP", e non quelle presenti nel tunnel, denominato "BRIDGE DATA".

Lo svantaggio di questa modalità è l'aver aggiunto un piccolo overhead ai pacchetti, che risulta trascurabile a fronte della semplicità di estensione e della elevata sicurezza che offre.

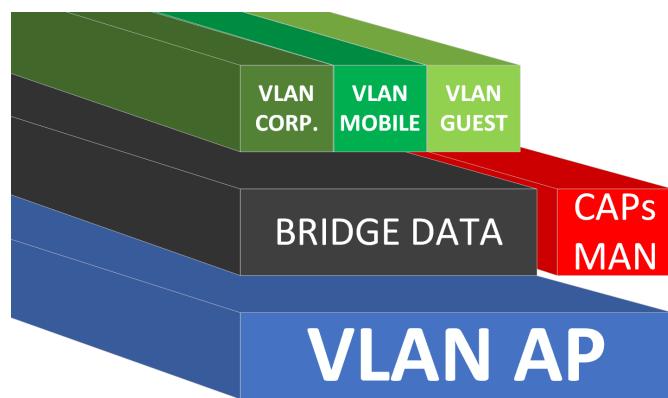


Figura 6.14: Configurazione della rete

6.3.5 Attivazione servizio NPS in Active Directory

Per consentire l'autenticazione tramite le credenziali Active Directory è stato predisposto il servizio NPS, in italiano denominato "criteri di rete".

Innanzitutto è stato abilitato il servizio NPS, per poi essere successivamente configurato. Si è poi proceduto con l'abilitazione del 802.1X, aggiungendo i clients RADIUS, che nel nostro caso è unicamente il MikroTik Cloud Core Router.

Prima di definire le politiche è stato creato un gruppo di utenti, il quale conterrà tutti coloro che avranno il privilegio di usufruire delle reti CORPORATE e MOBILE.

Le politiche di accettazione delle richieste possono essere riepilogate nel seguente modo:

1. Accetta se l'indirizzo IP appartiene alla rete Corporate, viene fornito il certificato corretto e le credenziali appartengono ad un utente inserito nel relativo gruppo;
2. Accetta se l'indirizzo IP appartiene alla rete Mobile e le credenziali appartengono ad un utente inserito nel relativo gruppo;
3. Rifiuta.

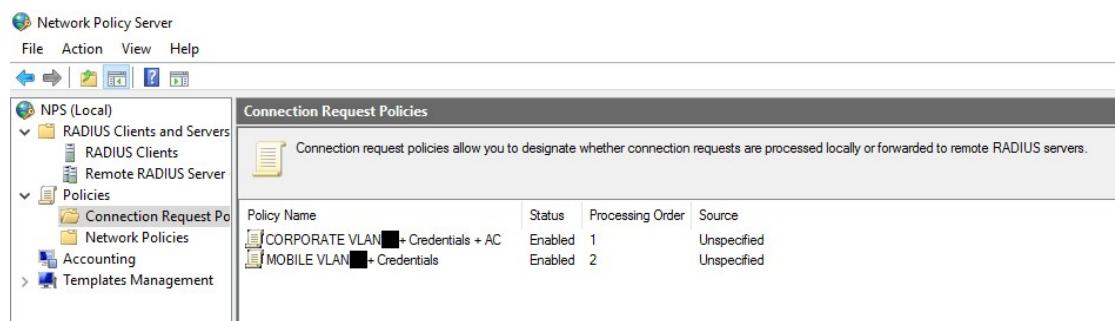


Figura 6.15: Politiche di sicurezza utilizzate

Successivamente le informazioni di accesso ai servizi NPS sono state inserite nella configurazione del Router MikroTik, in modo da permetterne la comunicazione tramite protocollo RADIUS.

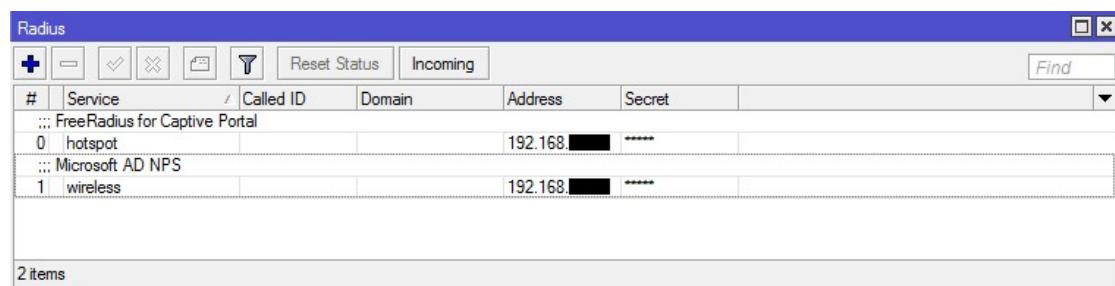


Figura 6.16: Configurazione RADIUS del controller MikroTik

6.3.6 Creazione del Captive Portal

La creazione del Captive Portal è stata effettuata su una macchina virtuale nuova, in modo tale da garantirne una segregazione nel sistema e delle regole nel firewall specifiche alla sua funzionalità.

Innanzitutto è stata effettuata l'installazione del sistema operativo CentOS 7, che è stato scelto perché già conosciuto ed ampiamente utilizzato nell'ambito aziendale. Successivamente si sono andati ad installare tutti i servizi, o "demoni" nello slang UNIX, in modo da offrire tutte le funzionalità richieste, brevemente riportati nella tabella sottostante.

Demone	Funzionalità	Utilizzo
HttpD	Servizio di server web, dedito alla gestione delle richieste http, risoluzione del codice PHP mediante apposito modulo ed invio di pagine web.	Gestione ed interazione dell'interfaccia del Captive Portal.
MySqlD	Servizio database, dedito al mantenimento e alla organizzazione dei dati, assieme al controllo d'accesso.	Gestione delle informazioni relative alla registrazione degli utenti, agli account abilitati e raccoglitrice di informazioni per RadD.
CronD	Servizio scheduler, dedito alla pianificazione dell'esecuzione dei comandi.	Controllo periodico degli account scaduti, che dovranno essere rimossi.
RadD	Servizio RADIUS, accede a una serie di direttive legate agli accessi e risponde in modo affermativo o negativo a delle richieste di autenticazione.	Utilizzato per determinare la validità degli account con i quali si effettua l'accesso nella rete.
FirewallD	Servizio firewall preinstallato in CentOS, determina quali connessioni sono permesse e quali invece devono essere bloccate.	Utilizzato per impedire un accesso dall'esterno ai servizi che non necessitano una iterazione dalla rete, ma solamente in locale, ad esempio MySqlD.

Demone	Funzionalità	Utilizzo
Sendmail	Servizio email, dedito al trasferimento di messaggi mediante SMTP.	Consente di inviare l'e-mail con la richiesta di approvazione allo sponsor e, in caso di accettazione, avvisa l'utente comunicandogli le informazioni necessarie all'accesso.

Tabella 6.1: Servizi per l'implementazione del Captive Portal

Sperimentazione Captive Portal sicuro

Durante la realizzazione del Captive Portal è stato deciso di effettuare un rapido test riguardante l'utilizzo di HTTPS con un certificato self-signed, in modo tale da impedire attacchi *Man In The Middle* durante l'autenticazione.

Purtroppo la modalità di redirezione utilizzata dagli hotspot è esplicitamente vietata nel protocollo HTTPS, però la sua implementazione varia secondo il produttore del sistema operativo.

Si è analizzato il comportamento su due dispositivi, un Huawei P8 con ROM EMUI e un Xiaomi Redmi 4X con ROM MIUI China Dev. EMUI, una volta connessa alla rete, rifiutava la risposta in HTTPS, in quanto violava lo standard, non rilevando quindi la presenza del captive portal ed impedendo all'utente di usufruire della navigazione. MIUI invece si comportava in modo più permissivo, ignorando l'infrazione del protocollo e presentando il login all'utente.

A causa di tali problematiche non si è proceduto all'abilitazione di HTTPS nel Captive Portal, mantenendo quindi la connessione in HTTP.

6.3.7 Inserimento regole Firewall

Una volta terminata la configurazione della rete è stato necessario, prima del suo utilizzo, inserire nuove regole all'interno del firewall per consentire il soddisfacimento dei requisiti relativi alle politiche di sicurezza precedentemente presentati. Tali regole potevano essere inserite anche nell'apparato Router di MikroTik, ma considerando la sua dotazione hardware si è preferito delegare il compito a dispositivi specifici, già presenti nel sistema.

Per eseguire tale operazione ho dovuto preparare la lista delle regole necessarie e comunicarle a chi di dovere affinché venissero applicate, in quanto mi era precluso l'accesso al firewall.

6.3.8 Test delle configurazioni in laboratorio

Prima di inserire il sistema in produzione si è andato a testare il funzionamento e la sua estensibilità.

Innanzitutto si è proceduto ad aumentare il numero di Access Point connessi in contemporanea, passando da 1 a 4, in modo tale da verificare la complessità della configurazione iniziale.

Per ogni nuovo dispositivo è stato sufficiente abilitare CAPsMAN sulle interfacce wireless affinché divenga operativo con tutte le misure di sicurezza abilitate.

Si è anche definita una password di accesso alla configurazione, che comunque non sarebbe stata raggiungibile da parte degli utilizzatori della connettività grazie al tunnel EoIP.

L’accesso ad internet si è rivelato funzionante e tutti i dispositivi venivano inseriti all’interno della VLAN con le corrispettive configurazioni fornite dal DHCP.

Test delle funzionalità di sicurezza in laboratorio

Un altro aspetto di elevata importanza è stata la sicurezza fornita dal nuovo sistema.

Innanzitutto si è verificata la stabilità del captive portal, cercando di forzare il login mediante attacchi *SQL injection* utilizzando SQLmap e VEGA.

I risultati ottenuti sono stati soddisfacenti, in quanto un preciso controllo dei valori inseriti all’interno dei campi di testo impediva di aggirare l’autenticazione.



Figura 6.17: Risultato ottenuto dalla analisi di VEGA

Successivamente si è andata a verificare la protezione ad eventuali attacchi eseguiti una volta già autenticati, come ad esempio il *Man In The Middle*. Non sono state rilevate vulnerabilità, in quanto gli altri dispositivi presenti nella rete risultavano irraggiungibili, e di conseguenza anche software come Wireshark e Arcai's NetCut non riuscivano a rilevare gli altri utenti. Una vulnerabilità implicita nel protocollo WiFi, impossibile da risolvere per la sua natura, è la cattura in monitor mode dei pacchetti che transitano sulla rete, permettendo quindi di identificare i dispositivi che usufruiscono della rete. Però anche questa vulnerabilità implicita risulta di scarsa utilità per un attaccante, in quanto la configurazione degli apparati non gli permettono di accedere agli altri dispositivi e manometterli.

Nella immagine sottostante si può notare a sinistra una analisi effettuata in una rete del cliente prima della installazione del nuovo sistema, con rilevati 29 dispositivi connessi, mentre a destra l'analisi effettuata nella nuova configurazione, senza nessun utente connesso visibile.

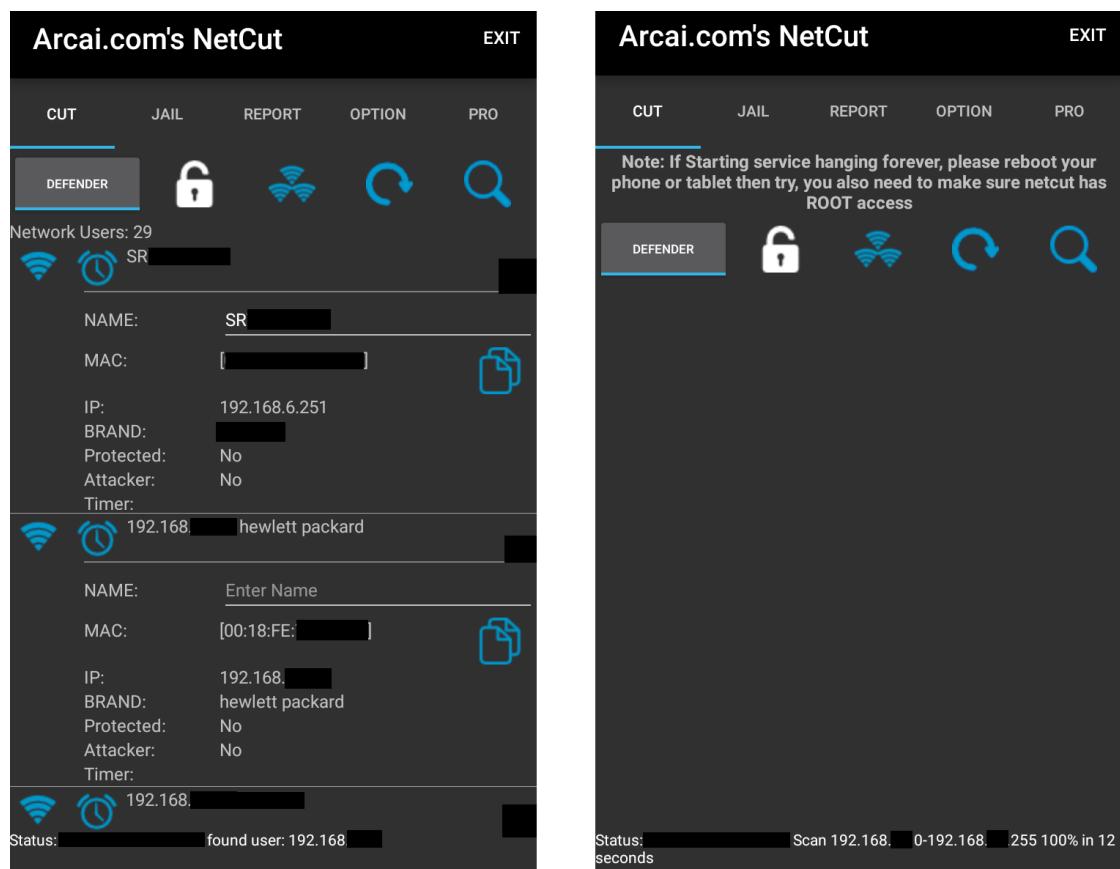


Figura 6.18: Risultati ottenuti con NetCut

6.3.9 Aggiornamento della documentazione progettuale

Durante questa fase è stata aggiornata la documentazione progettuale, andando a descrivere le funzionalità dei programmi e delle tecnologie utilizzate, il loro utilizzo e tutti i problemi riscontrati, correlati dalla soluzione applicata per correggerli.

6.4 Test finali

- **Periodo previsto:** dal 09/07/2018 al 13/07/2018;
- **Numero di ore previste:** 40h;
- **Periodo effettivo:** dal 12/07/2018 al 17/07/2018;
- **Numero di ore effettive:** 32h.

Il test in produzione non ha evidenziato gravi problematiche oppure problemi di progettazione, quindi le ore impiegate in questa attività sono state inferiori a quanto preventivato.

6.4.1 Individuazione problematiche

Le problematiche individuate si sono rilevate essere quantitativamente inferiori a quanto previsto. La maggior parte delle modifiche effettuate in questa fase sono state di piccola entità e mirate soprattutto a migliorare l'usabilità e l'interazione con gli utenti, come ad esempio migliorare la responsività dell'interfaccia del Captive Portal e migliorarne il testo.

Di seguito sono riportate le problematiche di maggior rilevanza.

Schedulazione automatica MikroTik non completata

Si è notato che la schedulazione dei backup di MikroTik non veniva eseguita, ma terminava inaspettatamente allo stabilimento della connessione FTP.

Analizzando la problematica si è scoperto che l'esecuzione manuale dello script veniva eseguita ignorando le sue policy, mentre l'esecuzione schedulata le rispettava. Il backup automatico possedeva già il permesso di utilizzare la connessione FTP, ma prima di stabilirla procedeva a controllare se la destinazione era raggiungibile, per tale motivo era richiesta anche la policy "test", che consentiva l'utilizzo del comando ping.

Adattabilità del Captive Portal a dispositivi mobili

Lo stile iniziale del Captive Portal prevedeva un footer con delle informazioni aggiuntive, ma lo stile ad esso assegnato era errato in quanto, utilizzando dispositivi con schermo particolarmente piccolo o con i caratteri grandi, andava a coprire il tasto di conferma del login.

Per correggere tale problema si è dovuto agire sul file CSS, facendo in modo tale che la parte in basso del sito non andasse mai a sovrapporsi con il contenuto.

6.4.2 Aggiornamento della documentazione progettuale

Durante questa fase è stata aggiornata la documentazione progettuale, andando a descrivere tutti i problemi riscontrati, correlati dalla soluzione applicata per correggerli.

6.5 Tuning

- **Periodo previsto:** dal 16/07/2018 al 27/07/2018;
- **Numero di ore previste:** 80h;
- **Periodo effettivo:** dal 18/07/2018 al 27/07/2018;
- **Numero di ore effettive:** 64h.

Questa fase ha visto come attività principali il potenziamento di Observium, espandendone le funzionalità attraverso un upgrade, configurandole e sfruttandole al meglio ed inserendo un sistema di alert tramite messaggi.

6.5.1 Upgrade Observium

Observium si è subito reso molto utile al monitoraggio della rete, questo ha portato alla decisione di acquistarne la versione professionale.

Le principali funzionalità offerte rispetto alla versione gratuita, definita Community, sono le seguenti:

- Update e fix costanti e non a cadenza di 6 mesi;
- Accesso alla repository SVN;
- Accesso alla versione beta;
- Raggruppamento dei dispositivi e delle interfacce in base alle loro caratteristiche;
- Metriche sulla qualità del servizio;
- Raggruppamento delle statistiche;
- Indicazione della tipologia degli errori di trasmissione;
- Ricerca di un dispositivo tramite IP o MAC address;
- Supporto da parte del team di sviluppo.

6.5.2 Allarmi Observium tramite E-mail e Telegram

Questa attività è stata eseguita nell’ultima fase in modo tale da consentirmi di aver compreso quali situazioni richiedono un avviso ed aver acquisito una sensibilità numerica riguardante i dati trattati.

Per poter utilizzare un sistema di avvisi automatici tramite messaggi è necessario prima definire le situazioni da considerare pericolose, definite come ”alert checks”. Ogni alerts check riguarda una classe di dispositivi, interfacce o sensori, come ad esempio le porte, i sensori di temperatura o i device stessi. Oltre al contesto si deve specificare, attraverso un metalinguaggio, i valori di soglia ed è possibile inserire dei filtri, in modo da escludere determinati dispositivi in base alle loro proprietà.

Name	Tests	Device Match / Entity Match	Entities
ALERT - Banda ponte radio ALERT - Banda ponte radio	ifInOctets_perc >= 65 ifOperStatus == up	* port_id in 7673,7674,9661,7731	4 4 0 0 0 0
ALERT - Banda usata fibra ALERT - Banda usata su fibra	ifInOctets_perc > 65 ifOperStatus == up	* ifHighSpeed == 1000 ifTrunk == dot1Q	195 165 0 0 0 30
ALERT - Banda usata fibra 10G ALERT - Banda usata fibra 10G	ifInOctets_perc >= 65 ifOperStatus == up	* ifHighSpeed == 10000	14 14 0 0 0 0
Device Down Notifica sulla raggiungibilità del dispositivo	device_status equals 0	* *	94 89 5 0 0 0
Port down Notifica sullo stato di una porta	ifAdminStatus == up ifOperStatus != up	* ifType == ethernetCsmacd	1373 577 31 0 0 765
Port lost packages Notifica messaggi persi da una porta	ifInDiscards_rate > 80 ifOutDiscards_rate > 80	* ifType equals ethernetCsmacd	1373 607 0 0 0 766
Port with errors Notifica errori nei messaggi da una porta	ifInErrors_rate > 15 ifOutErrors_rate > 15	* ifType equals ethernetCsmacd	1373 607 0 0 0 766
Problema alimentazione Notifica di errore nella alimentazione	sensor_value greater @sensor_limit sensor_value less @sensor_limit_low	* sensor_class equals power	194 194 0 0 0 0
Problema amperaggio Notifica di problema nell’amperaggio	sensor_value greater 160 sensor_value less @sensor_limit_low	* sensor_class equals current	114 114 0 0 0 0
Problema voltaggio Notifica di errore nel voltaggio	sensor_value greater @sensor_limit sensor_value less @sensor_limit_low	* sensor_class equals voltage	114 114 0 0 0 0
Stato a warning Notifica di warning ricevuto da un dispositivo	status_event equals warn	* *	272 272 0 0 0 0
Stato ad alert Notifica di alert ricevuto da un dispositivo	status_event equals alert	* *	272 272 0 0 0 0
WARNING - Banda ponte radio WARNING - Banda ponte radio	ifInOctets_perc >= 50 ifInOctets_perc < 65 ifOperStatus == up	* port_id in 7673,7674,9661,7731	4 4 0 0 0 0
WARNING - Banda usata fibra WARNING - Banda usata sulla fibra	ifInOctets_perc >= 50 ifInOctets_perc < 65 ifOperStatus == up	* ifHighSpeed == 1000 ifTrunk == dot1Q	195 165 0 0 0 30
WARNING - Banda usata fibra 10G WARNING - Banda usata fibra 10G	ifInOctets_perc >= 50 ifInOctets_perc < 65 ifOperStatus == up	* ifHighSpeed == 10000	14 14 0 0 0 0

Figura 6.19: Alert checks creati in Observium

Successivamente sono stati inseriti dei contatti, sia E-mail che identificativi di conversazioni con un bot di *Telegram_G*, e relativamente ad ognuno di essi sono stati abilitati gli alert che interessavano al destinatario.

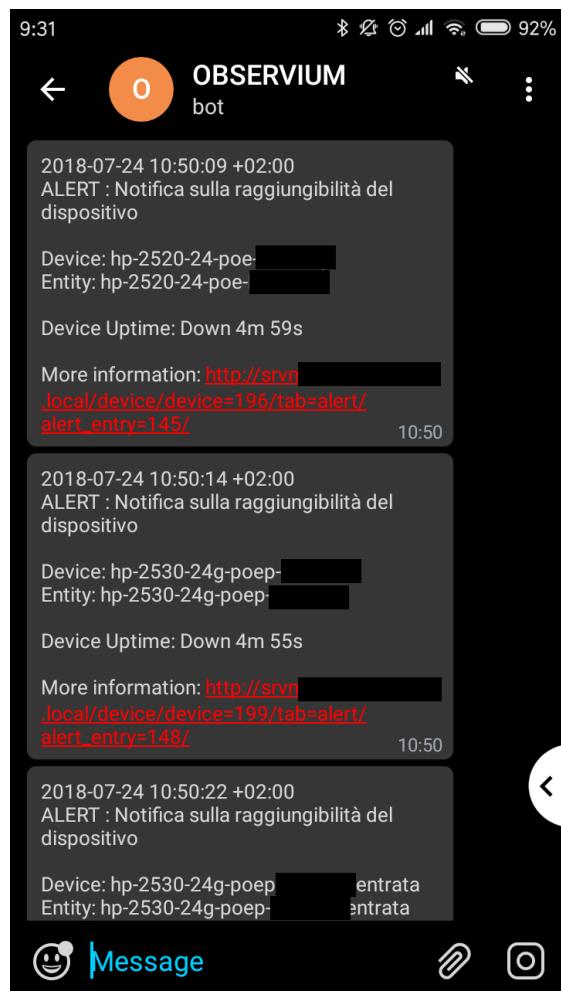


Figura 6.20: Screenshot degli avvisi nell'applicazione Telegram

6.5.3 Raggruppamento delle interfacce

Per velocizzare l'analisi della rete è stato ritenuto utile poter consultare lo stato di più interfacce contemporaneamente, per tale ragione si è andato ad utilizzare la funzionalità di raggruppamento delle porte offerto da Observium.

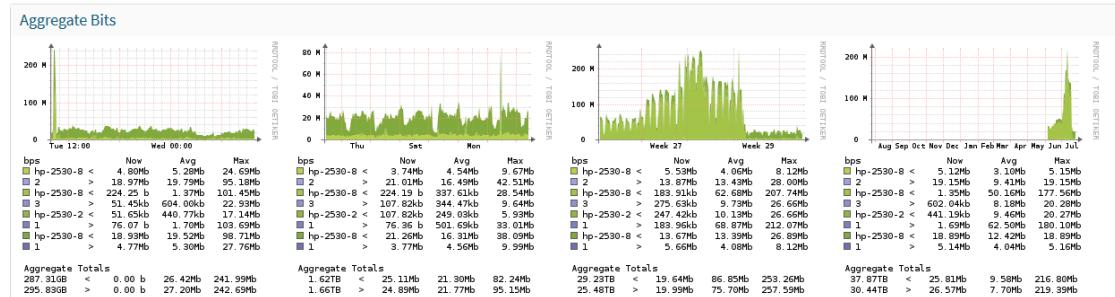


Figura 6.21: Stato dell'utilizzo del ponte radio

Un esempio è il gruppo delle interfacce sulle quali comunicano il ponte radio. Questo è utile per poter identificare eventuali problemi nel resto della rete, in quanto la connessione wireless a lungo raggio è stata delegata come supporto alla rete cablata ed eventuale backup, quindi se il traffico totale aumenta notevolmente significa che sono presenti delle problematiche.

6.5.4 Raggruppamento dispositivi

Vista la quantità elevata di dispositivi si è deciso di utilizzare il raggruppamento offerto da Observium per categorizzarli.

L'operazione è stata molto veloce, in quanto il software permette di effettuare questa operazione in modo automatico attraverso condizioni e espressioni regolari. Questo consente anche un update automatico dei gruppi in caso di eliminazione o di aggiunta di nuovi dispositivi.

6.5.5 Completamento della documentazione

Prima di terminare l'attività di stage è stata completata la documentazione, in modo tale da aggiornarla per illustrare le ultime attività effettuate ed indicare le operazioni atte alla sua manutenzione.

Capitolo 7

Valutazione retrospettiva

7.1 Tempo impiegato

7.1.1 Riepilogo tempo impiegato

Descrizione attività	Durata prevista	Durata effettiva
Analisi	40h	40h
Progettazione	80h	96h
Implementazione	80h	88h
Test	40h	32h
Tuning	80h	64h

Tabella 7.1: Tempo previsto ed impiegato

7.1.2 Considerazioni sugli scostamenti

Durante l'esecuzione delle attività sono avvenuti degli scostamenti temporali su quanto preventivato. Le cause sono principalmente da ricercarsi sull'utilizzo di tecnologie a me poco conosciute, che mi hanno impedito di determinare con precisione i tempi.

Grazie però ad una estesa analisi preliminare delle tecnologie ed a una buona progettazione non è stato dispendioso metterci mano successivamente per rendere il risultato pronto alla produzione, consentendomi quindi di terminare l'attività senza aver tralasciato nulla di quanto pianificato inizialmente.

7.2 Risultati ottenuti

7.2.1 Soddisfacimento risultati attesi

Di seguito sono riportati i risultati ottenuti a fine stage.

Monitoraggio

Misurazione	Valore minimo accettato	Valore massimo accettato	Valore ottenuto
Tempo medio di composizione di una pagina	0ms	500ms	395ms
Numero di dispositivi di rete monitorati in contemporanea	80	-	94
Numero di interfacce monitorate in contemporanea	2500	-	3064
Numero di sensori e periferiche monitorati in contemporanea	500	-	724
Numero di alert checks presenti	10	20	15
Protezione delle informazioni tramite password	Si	-	Si

Tabella 7.2: Risultati ottenuti per l'implementazione di Observium

Gestione delle configurazioni dei dispositivi di rete

Misurazione	Valore minimo accettato	Valore massimo accettato	Valore ottenuto
Tempo di composizione di una pagina	0ms	100ms	32ms
Numero di dispositivi di rete gestiti in contemporanea	80	-	87
Protezione delle informazioni tramite password	Si	-	Si

Tabella 7.3: Risultati ottenuti per l'implementazione di rConfig

Politiche di sicurezza

Misurazione	Valore richiesto	Valore ottenuto
Possibilità per gli impiegati di usufruire dei servizi locali alla rete (stampanti, fax)	Si	Si
Possibilità per gli impiegati di usufruire dei servizi remoti (accesso ai database, relay email)	Si	Si
Possibilità per gli impiegati di accedere ad internet attraverso protocolli definiti	Si	Si
Possibilità per i dispositivi mobili del personale di usufruire dei servizi locali alla rete (stampanti, fax)	No	No
Possibilità per i dispositivi mobili del personale di usufruire dei servizi remoti (accesso ai database, relay email)	No	No
Possibilità per i dispositivi mobili del personale di accedere ad internet attraverso qualsiasi protocollo	No	No
Possibilità per i dispositivi mobili del personale di accedere ad internet attraverso i protocolli HTTP, HTTPS, SMTP, SMTPL, POP3, POP3S, IMAP, IMAPS, IPSEC VPN	Si	Si
Necessità per i dispositivi mobili del personale di effettuare una autenticazione tramite Captive Portal	No	No
Possibilità per gli ospiti di usufruire dei servizi locali alla rete (stampanti, fax)	No	No
Possibilità per gli ospiti di usufruire dei servizi remoti (accesso ai database, relay email)	No	No
Possibilità per gli ospiti di accedere ad internet attraverso qualsiasi protocollo	No	No
Possibilità per gli ospiti di accedere ad internet attraverso i protocolli HTTP, HTTPS, SMTP, SMTPL, POP3, POP3S, IMAP, IMAPS, IPSEC VPN	Si	Si
Necessità per gli ospiti di effettuare una autenticazione tramite Captive Portal	Si	Si

Tabella 7.4: Risultati ottenuti per l'implementazione delle politiche di sicurezza

Captive Portal

Misurazione	Valore richiesto	Valore ottenuto
Possibilità di effettuare il login	Si	Si
Possibilità di registrazione tramite sponsor	Si	Si
Registrazione valida per un determinato periodo di tempo	Si	Si
Interfaccia utilizzabile da un dispositivo mobile	Si	Si
Registrazione tramite e-mail	Si	Si
Possibilità di registrazione con e-mail altrui	No	No
Sezione di amministrazione facilmente accessibile	Si	Si
Sezione di amministrazione protetta da password	Si	Si
Funzionalità di gestione degli sponsor	Si	Si
Funzionalità di gestione degli account	Si	Si
Funzionalità di gestione delle durate temporali	Si	Si

Tabella 7.5: Risultati ottenuti per l'implementazione del Captive Portal

7.2.2 Risultati aziendali

Monitoraggio della rete

Al termine dello stage la rete è stata posta sotto monitoraggio in ogni sua parte, consentendo di ottenere informazioni, statistiche e segnalazioni in tempo reale.

Versioning delle configurazioni dei dispositivi

Le impostazioni dei dispositivi, che erano precedentemente perdute se accadeva un guasto del dispositivo, sono ora periodicamente salvate e mantenute in un ambiente sicuro, permettendo un rapido ripristino della configurazione su una nuova macchina nel caso ci sia la necessità di sostituzione.

Nuovo sistema di Access Point

Gli access point precedenti, prodotti per utenti casuali e quindi di scarse funzionalità, sono ora stati sostituiti da dispositivi più performanti, più sicuri e più manutenibili.

Con il nuovo sistema adottato è anche possibile estendere, con una minima configurazione, la rete, mantenendone la sicurezza e le caratteristiche.

Politiche di sicurezza

Il vecchio sistema di autenticazione nel WI-FI, che consisteva nell'utilizzo di una password unica per tutti, dall'ospite al dirigente, è stato completamente rivisto.

Sono state introdotte più reti, ognuna con una classe di utenti ben definiti, e le politiche di sicurezza e di autenticazione sono state concepite secondo le necessità degli utilizzatori delle rispettive reti.

Creazione di un captive portal

Per consentire un tracciamento degli ospiti, impedire la diffusione delle password di accesso e scoraggiarne l'utilizzo da parte dei dipendenti è stato creato un captive portal a sostegno dell'autenticazione della rete Guest.

Il prodotto finale offre all'amministratore un pannello di controllo, in modo che possa modificare autonomamente le informazioni in esso raccolte, senza dover accedere manualmente alla base di dati.

7.2.3 Sviluppi futuri

L'attività svolta ha portato ad un drastico incremento della sicurezza nella rete, che però si è limitata, per motivi di tempo, solamente ad alcuni ambiti.

A fronte del lavoro svolto, soprattutto in riferimento all'implementazione della rete WiFi con 802.1X e NPS, si sono stese delle solide basi per estendere ulteriormente la sicurezza. Un possibile progetto, impegnativo ed impattante sulla configurazione di tutta la rete, sarebbe l'implementazione del protocollo 802.1X sulla rete cablata. Questo porterebbe a un miglioramento aggiuntivo di notevole importanza alla sicurezza fisica della rete.

7.2.4 Risultati personali

Approfondimento del funzionamento di una rete Campus Area Network

Grazie all'attività offertami ho potuto interagire sul campo con gli apparati di rete, che avevo precedentemente studiato attraverso la certificazione Cisco in mio possesso e i corsi universitari da me frequentati.

Questo mi ha fatto comprendere molti aspetti che ignoravo, come l'importanza di avere la ridondanza nelle connessioni, le criticità provocate dai colli di bottiglia e la velocità con la quale l'utilizzo della rete può cambiare in concomitanza a particolari momenti della giornata od eventi sociali.

Comprendere delle principali problematiche di una rete di grandi dimensioni

Lavorando a contatto con una rete di dimensioni così considerevoli ho potuto apprendere quali sono le principali problematiche. Questo mi ha fatto capire che la probabilità di guasti è molto bassa per ogni singolo componente, ma considerando l'estensione della rete risultano frequenti.

Le cause principali delle disconnessioni degli apparati sono da attribuirsi a problemi della distribuzione della corrente elettrica, che in ambienti vasti e con un elevato numero di persone è frequente.

Una seconda problematica sono i guasti hardware, legati principalmente all'alimentazione PoE delle porte, all'alimentazione del dispositivo o agli iniettori di corrente PoE, mentre le componenti che potrebbero essere considerate più complesse, come gli elaboratori o gli switch chip, sono molto meno inclini a problemi.

Apprendimento dell'importanza del monitoraggio

Grazie all'attività svolta ho potuto constatare anche quanto frequentemente le problematiche presenti in una rete non sono neppure rilevate, e rimangono tali fino a quando non portano a disservizi.

In particolare ho individuato, mediante l'aiuto di Observium, la presenza di 3 switch che presentavano il PoE in uno stato di Fault, il quale non era segnalato su PRTG e non veniva neppure evidenziato nell'interfaccia web del dispositivo.

Apprendimento tecnologie per il proseguimento della sicurezza

Durante il corso di reti ho potuto apprendere svariate metodologie e tecnologie utilizzate per il conseguimento della sicurezza, però molte di esse non erano state analizzate durante le lezioni a causa della vastità dell'argomento e della durata del corso.

Questo stage mi ha dato la possibilità di utilizzare molte tecnologie che avevo studiato o che neppure conoscevo, ed ho potuto anche comprendere quali vulnerabilità mirano a correggere e le loro modalità di utilizzo.

Apprendimento della creazione e configurazione di macchine Linux

Durante l'attività universitaria si mira ad imparare l'utilizzo del linguaggio PHP e di MySQL, ma la sua installazione viene lasciata agli studenti, la quale viene solitamente effettuata mediante l'utilizzo di bundle, come ad esempio XAMPP, senza approfondire i componenti che contiene e le loro configurazioni.

Nell'ambito dello stage era ovvio fino da subito che non potevo seguire questa metodologia, in quanto ogni impostazione doveva essere sicura e la macchina non doveva contenere servizi aggiuntivi inutilizzati.

Per tale motivo si sono andate a creare delle macchine virtuali Linux, nello specifico CentOS, sulle quali ho installato e configurato manualmente tutti e soli i servizi necessari per offrire in modo sicuro, continuativo ed efficiente i servizi richiesti.

Questa attività mi ha fatto comprendere molte best practice relative alla configurazione dei servizi di rete.

Miglioramento della capacità di scripting e manipolazione dei dati

Grazie alla mole dei dati da inserire all'interno dei vari software ho messo mano ad alcune tecnologie viste durante svariati corsi universitari.

Per l'elaborazione dei dati ho avuto modo di confrontarmi con le espressioni regolari e con il linguaggio JavaScript, utilizzato mediante GreaseMonkey.

Questo mi ha permesso di svolgere nel giro di alcune ore una mole di lavoro che, se svolta manualmente, poteva impiegare fino ad alcune giornate.

7.3 Vincoli del progetto

7.3.1 Vincoli tecnologici

Statistiche VLAN

Una limitazione tecnologica attualmente presente in Observium è la sua incapacità di creare dei raggruppamenti in base alla VLAN utilizzata.

Questo fatto, in concomitanza agli switch utilizzati che non permettevano la raccolta di statistiche dalle interfacce virtuali, comprendenti le VLAN, ha impedito di ottenere statistiche sull'utilizzo della rete suddivise per rete virtuale.

La limitazione non si sarebbe presentata con l'adozione di switch Cisco, in quanto essi raccolgono informazioni suddividendoli anche per VLAN, che possono poi essere raggruppati con facilità su Observium.

L'informazione che si sarebbe dovuta utilizzare per il raggruppamento delle porte fisiche è già presente all'interno del database dell'applicazione, ed è già possibile utilizzarla per creare un filtro sugli avvisi, ma non è ancora stata implementata per il raggruppamento.

Supporto MikroTik in rConfig

Una problematica emersa durante la configurazione dei backup automatici dei dispositivi è stata l'impossibilità di utilizzare rConfig per i dispositivi MikroTik. Questa problematica deriva probabilmente dal fatto che il sistema di MikroTik, denominato RouteOS, invia sui terminali anche caratteri speciali per il colore del testo, i quali sono male interpretati da rConfig. Questo impedisce al programma di svolgere la sua funzionalità, in quanto non riesce a comprendere le risposte che gli vengono fornite dall'apparato.

Infine il log generato dall'applicazione era poco verboso, che in accoppiata ad una progettazione non di elevato livello andava ad aumentare la difficoltà nella individuazione di una eventuale patch. Per tale motivo si è scelto di proseguire per una via alternativa, delegando i singoli dispositivi ad effettuare autonomamente un backup ed a salvarlo in remoto, piuttosto che mettere mano al codice sorgente del programma.

Utilizzo di SSL nel Captive Portal

Per aumentare la sicurezza della rete si è anche analizzata la possibilità di utilizzare HTTPS supportato da certificati digitali SSL self signed per il Captive Portal. Purtroppo questa pratica non è permessa dallo standard HTTPS nell'ambito dei Captive Portal, in quanto il protocollo mira ad impedire redirezioni forzate dell'utente, compresa quella necessaria per essere portati alla pagina di autenticazione.

Molti dispositivi, soprattutto mobili, per verificare la presenza dei Captive Portal inviano una richiesta http ad un server e individuano se la risposta è corretta oppure se c'è stata un redirezione, procedendo quindi ad avvisare l'utente e a visualizzare la pagina che hanno ricevuto. Se la risposta avviene mediante HTTPS allora sarà errato rispetto a quanto richiesto, solitamente portando ad ignorare l'intera procedura. Questo impedisce di rilevare il portale, quindi l'utente non potrà effettuare il login ed utilizzare la rete.

7.3.2 Vincoli temporali

Fortunatamente non si sono presentati vincoli riguardanti la durata dell'attività, in quanto, seppur alcune attività avessero impiegato un tempo maggiore a quanto preventivato, complessivamente il numero di ore concessomi è stato sufficiente a terminare tutti gli obiettivi posti inizialmente.

Appendici

Appendice A: Schemi di rete

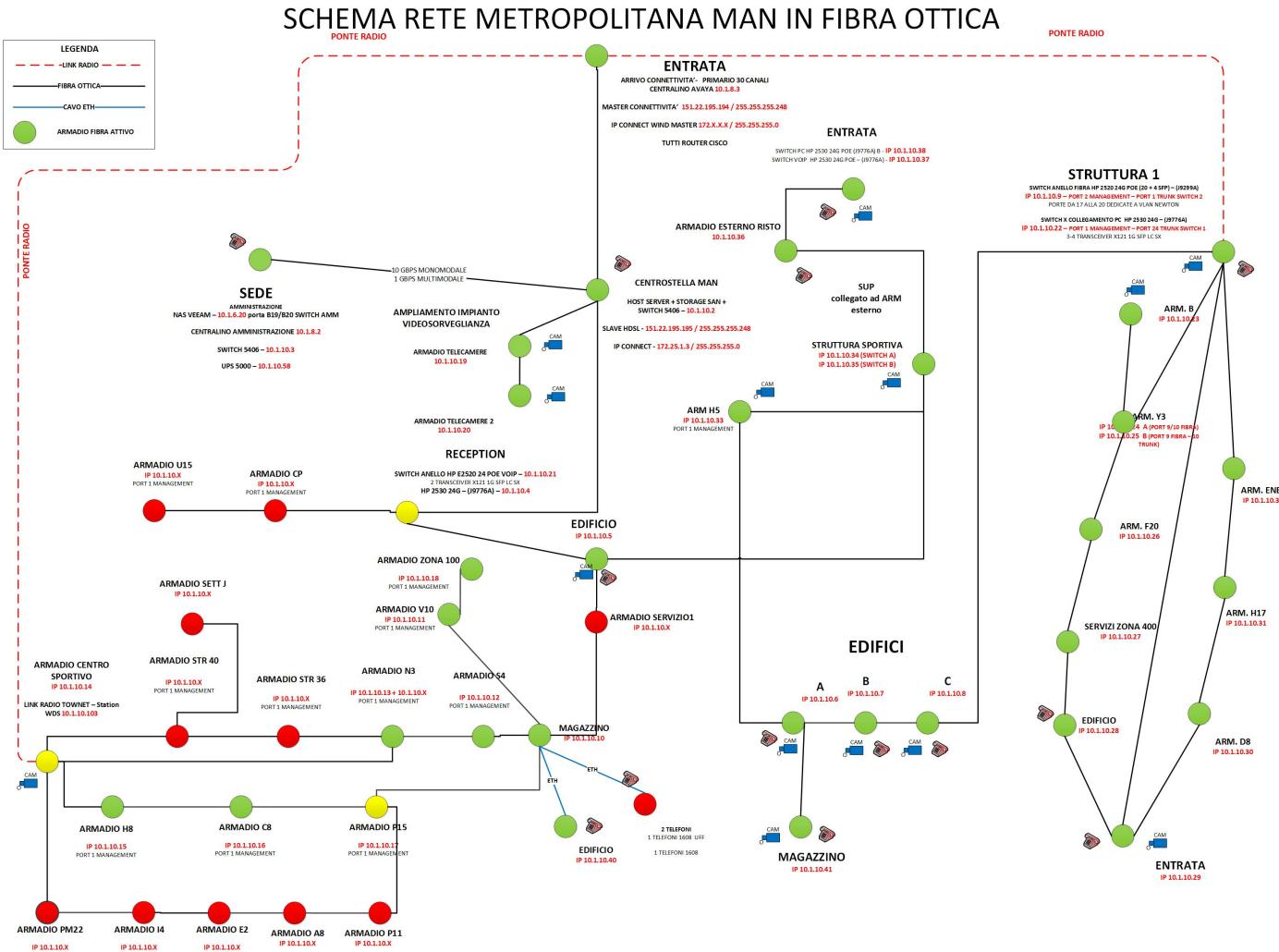


Figura 7.1: Schema Visio della rete datato 2015

Monitoraggio e sicurezza fisica di reti LAN Campus

70

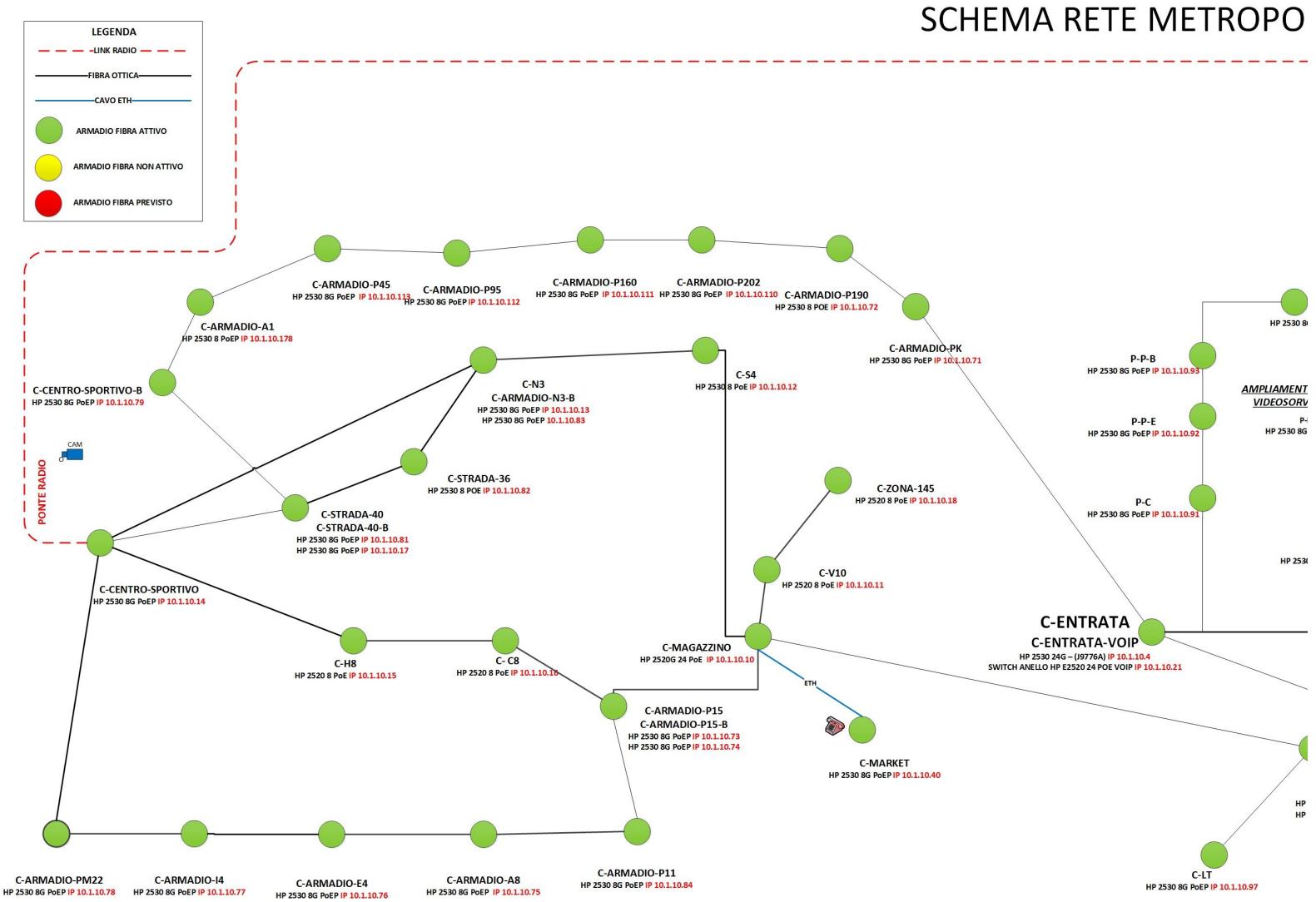


Figura 7.2: Schema Visio della rete a fine stage, prima parte

Appendix

LITANA MAN IN FIBRA OTTICA

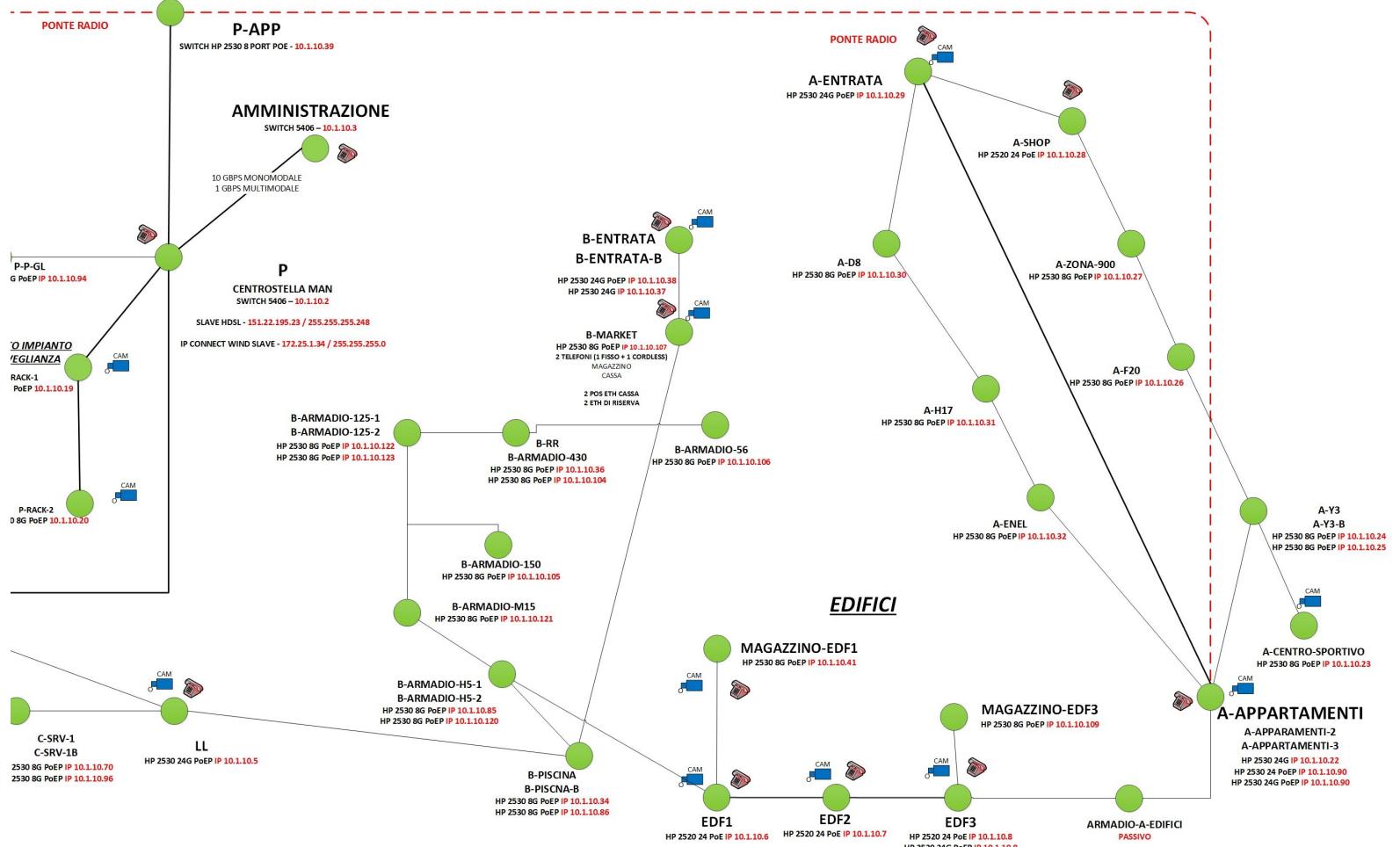


Figura 7.3: Schema Visio della rete a fine stage, seconda parte

Appendice B: Script di popolamento rConfig

Il codice sotto riportato è uno script in linguaggio JavaScript per il popolamento automatico, una volta inseriti i dati, di rConfig.

Lo script può essere utilizzato mediante il plug-in GreaseMonkey versione 4.0 o successive, in quanto richiede l'archiviazione di un valore nella memoria dell'estensione per funzionare.

```

1 // ==UserScript==
2 // @name      auto-insert-devices-rConfig
3 // @namespace MircoCailottoWintech
4 // @include   https://INDIRIZZO_RCONFIG/devices.php
5 // @version   1
6 // @grant     GM.setValue
7 // @grant     GM.getValue
8 // ==/UserScript==
9
10 // DATA
11
12 const data = [
13 ["INDIRIZZO-DISPOSITIVO-IN-DNS", "", "ENABLE-PROMPT#", "MARCA", "",
14   "MODELLO", "GRUPPO", "LOCAZIONE", "TEMPLATE_DI_RECUPERO_DATI"],
15 ["HP3850-24G-POE-C-ARMADIO-S123", "", "ARMADIO-S123#", "HP", "",
16   "HP3850-24G-POE", "SwitchesHP", "ClienteA", "HP Procurve SSH no
17   enable - HP-Procurve-SSH-no-enable.yml"],
18 ["HP3850-24G-POE-C-ARMADIO-C23", "", "C-ARMADIO-C23#", "HP", "",
19   "HP3850-24G-POE", "SwitchesHP", "ClienteA", "HP Procurve SSH no
20   enable - HP-Procurve-SSH-no-enable.yml"],
21 ];
22
23 function insertData(index) {
24   document.getElementById('deviceName').value = data[index][0];
25   document.getElementById('deviceEnablePrompt').value = data[index]
26     [1];
27   document.getElementById('devicePrompt').value = data[index][2];
28
29   var select = document.getElementById('vendorId');
30   for (var i = 0; i < select.options.length; i++) {
31     if (select.options[i].text === data[index][3]) {
32       select.selectedIndex = i;
33       break;
34     }
35   }
36
37   document.getElementById('deviceModel').value = data[index][4];
38 }
```

```

34     select = document.getElementById('catId');
35     for (var i = 0; i < select.options.length; i++) {
36       if (select.options[i].text === data[index][5]) {
37         select.selectedIndex = i;
38         break;
39     }
40   }
41
42   document.getElementById('custom_Location').value = data[index]
43     [6];
44
45   select = document.getElementById('templateId');
46   for (var i = 0; i < select.options.length; i++) {
47     if (select.options[i].text === data[index][7]) {
48       select.selectedIndex = i;
49       break;
50     }
51
52 //LOGIN
53   document.getElementById('defaultCreds').checked = true;
54 // document.getElementById('deviceUsername').value = "username";
55 // document.getElementById('devicePassword').value = "password";
56 // document.getElementById('deviceEnablePassword').value =
57   "passwordroot";
58 };
59
60 function clickOkButton() {
61   setTimeout(function(){
62     unsafeWindow.resolveDevice(document.getElementById('deviceName'
63       ).value);
64     setTimeout(function(){
65       document.getElementById("submit").click();
66     }, 500);
67   }, 500);
68 }
69
70 window.addEventListener('load', function() {
71   // once loaded
72   (async () => {
73     console.log("Async call");
74
75     // ----- RESET THE SCRIPT -----
76     var reset = false;
77
78     if(reset) {
79       GM.setValue('count', 0);
80     } else {
81       var index = await GM.getValue('count', 0);
82     }
83   });
84 }

```

```
80     if(index < data.length) {
81         //insert
82         console.log("Adding item number:");
83         console.log(index);
84         insertData(index);
85         GM.setValue('count', index + 1);
86         clickOkButton();
87     } else {
88         //done, do nothing
89         console.log("Already done");
90     }
91 }
92 }
93 })();
94 }, false);
```

Listing 7.1: Script GreaseMonkey di popolamento rConfig

Le linee 13, 14 e 15 sono 3 apparati che saranno inseriti alla esecuzione dello script, i campi sono:

1. Indirizzo DNS del dispositivo
2. Prompt del dispositivo in modalità non privilegiata, opzionale
3. Prompt del dispositivo in modalità privilegiata
4. Marca del dispositivo
5. Modello del dispositivo
6. Gruppo rConfig di appartenenza del dispositivo, utilizzabile per il filtraggio
7. Locazione del dispositivo, utilizzabile per il filtraggio
8. Template rConfig relativo alla configurazione da utilizzare per il recupero dei dati

Le linee 54, 55 e 56 presentano la possibilità di specificare i parametri per effettuare il login ai dispositivi, attualmente non utilizzati in quanto si utilizza le credenziali impostate come di default.

La linea 74 presenta un variabile "reset" che se impostata a true, invece che eseguire lo script, va ad azzerare i valori utilizzati dal plugin, permettendone una seconda esecuzione.

Appendice C: Script di backup Mikrotik

Di seguito è riportato lo script eseguito e schedulato sui dispositivi MikroTik, sia di tipologia router che access point. La sua esecuzione consiste nella generazione automatica di un file di backup delle impostazioni e il suo salvataggio su server FTP_G remoto.

```

1 # ----- Configuration -----
2 # FTP server address
3 :local ftp_server_address backupmikrotik.ftpserver.local
4 # FTP username
5 :local ftp_username ftp_username
6 # FTP password
7 :local ftp_password ftp_password
8 # remote directory
9 :local remote_directory /backupMikroTik/Router/
10 # name of the file, without the date
11 :local file_name ExportMikrotikSettingsController
12
13 # ----- Create strings -----
14 # Get the date
15 :local ts [/system clock get time]
16 :set ts ([:pick $ts 0 2]."-".[:pick $ts 3 5]."-".[:pick $ts 6 8])
17 :local months {"jan"="01";"feb"="02";"mar"="03";"apr"="04";"may"=
    "05";"jun"="06";"jul"="07";"aug"="08";"sep"="09";"oct"="10";"nov"=
    "11";"dec"="12"};
18 :local ds [/system clock get date]
19 :local mm (:$months->[:pick $ds 0 3])
20 :set ds ([:pick $ds 7 11]."$mm-".[:pick $ds 4 6])
21
22 # Add the automatic extension to the filename
23 :set backupFileName "$backupFileName.rsc"
24
25 # Compose the remote path
26 :set remoteBackupFileName "$remote_directory$backupFileName.rsc"
27
28 # Compose the filename
29 :local backupFileName "$file_name-$ds-$ts"
30
31 # ----- Execute the backup -----
32 # Export the configuration
33 /export file=$backupFileName
34
35 # Upload the file to the ftp server
36 /tool fetch mode=ftp address=$ftp_server_address port=21 user=
    $ftp_username password=$ftp_password src-path=$backupFileName
    dst-path=$remoteBackupFileName upload=yes
37

```

```
38 # Remove the file from the device  
39 /file remove $backupFileName
```

Listing 7.2: Script per il backup dei device MikroTik

Alla riga 3, 5 e 7 sono dichiarate le informazioni di accesso FTP al server dedito al mantenimento dei backup, mentre nella riga 9 viene indicata la cartella remota sulla quale inserire il file.

Alla riga 11 viene definito il nome che assumerà il file di backup, con omesse le informazioni sulla data, che saranno aggiunte automaticamente.

Lo script, che si suppone sia stato nominato "script_backup_ftp", può essere aggiunto alla schedulazione automatica mediante il seguente comando.

```
1 /system scheduler  
2 add  
3   name=scheduler_backup_ftp \  
4   interval=1w \  
5   start-date=jan/01/2018 \  
6   start-time=03:00:00 \  
7   on-event="/system script run script_backup_ftp" \  
8   policy=ftp,read,write,policy,password,sensitive,test
```

Listing 7.3: Comando per la schedulazione del backup

In questo modo lo script verrà eseguito ogni lunedì alle 3:00 del mattino, in quanto il 1 gennaio 2018 è un lunedì e la cadenza sarà settimanale.

Glossario

Captive portal

Un Captive portal è una pagina web che viene mostrata agli utenti di una rete di telecomunicazioni quando tentano di connettersi ad Internet mediante una richiesta http del loro browser.

CSV

Il formato CSV, ovvero Comma-Separated Values, è basato su file di testo composti da righe presentanti valori separati da una virgola. Non esiste uno standard formale che lo definisca, ma solamente alcune prassi più o meno consolidate.

Domain Controller

Un Domain Controller (DC) è un server che, nell'ambito di un dominio, attraverso Active Directory (AD), gestisce le richieste di autenticazione per la sicurezza e organizza la struttura del dominio in termini di utenti, gruppi e risorse di rete fornendo dunque un servizio di directory service.

EAPoL

EAP over Lan, abbreviato in EAPoL, è un protocollo di rete generico che permette di incapsulare il protocollo EAP per essere trasmesso.

Espressione regolare

Una espressione regolare, in inglese Regular Expression, Regex o RE, è una sequenza di simboli che identifica un insieme di stringhe. Essa costituisce una funzione che prende in ingresso una stringa e ne restituisce una seconda.

FTP

Il protocollo FTP, per esteso File Transfer Protocol, permette la trasmissione di dati tra host. Funziona sul protocollo TCP ed utilizza una architettura client-server, anche se è possibile trasferire dati anche tra server.

Man In The Middle

L'attacco Man In The Middle, spesso indicato con "MITM", consiste nella modifica delle tabelle ARP degli apparati di rete al fine di inserirsi in una comunicazione. Questo consente all'attaccante di analizzare il traffico del dispositivo ed eventualmente manometterlo.

Quality Of Service

La qualità del servizio, documentata mediante *RFC_G*, è la descrizione o la misurazione delle performance di un servizio di rete, secondo la visione da parte dell'utente a seconda della possibile attività che sta svolgendo.

RADIUS

Il protocollo di rete RADIUS fornisce una autenticazione centralizzata ed opera sulla porta 1812. Viene spesso utilizzato con 802.1X. Con il termine RADIUS si può indicare anche il server che fornisce il servizio di autenticazione mediante questo protocollo.

RFC

Un RFC o Request For Comments, in italiano "richiesta di commenti", è un documento pubblicato dalla Internet Engineering Task Force, che riporta informazioni riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico.

Sicurezza fisica

Per sicurezza fisica si intendono il complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, dispositivi, apparati, informazioni e dati di natura riservata.

Sicurezza logica

Per sicurezza logica si intendono il complesso di soluzioni che impediscono ad utenti non autorizzati di compiere azioni che richiedono dei privilegi più elevati rispetto a quelli in loro possesso.

SQL injection

SQL injection è una tecnica di code injection, usata per attaccare applicazioni di gestione dati, con la quale vengono inserite delle stringhe di codice SQL malevole all'interno di campi di input. .

System Integrator

Con il termine System Integrator viene indicata una azienda che si occupa di far dialogare impianti diversi tra di loro allo scopo di creare una nuova struttura funzionale che possa utilizzare le potenzialità di impianti d'origine e creare quindi funzionalità originariamente non presenti.

Telegram

Telegram è un servizio di messaggistica istantanea basato su Cloud. Le caratteristiche di Telegram sono la possibilità di stabilire conversazioni cifrate punto-punto, effettuare chiamate vocali cifrate, scambiare messaggi vocali, videomessaggi, fotografie, video, stickers e file di qualsiasi tipo.

Bibliografia

Documenti in lingua italiana

- Portale di Clusit, associazione per la sicurezza informatica
<https://clusit.it>
- Introduzione a CentOS 7
<http://www.html.it/articoli/centos-7-una-distro-enterprise-gratuita>
- Guida a Systemd
[https://wiki.archlinux.org/index.php/Systemd_\(Italiano\)](https://wiki.archlinux.org/index.php/Systemd_(Italiano))

Documenti in lingua inglese

- Documentazione Observium
<http://docs.observium.org>
- Documentazione Microsoft relativa a Active Directory
<https://docs.microsoft.com/en-us/windows-server/identity/identity-and-access>
- Presentazione MikroTik - WiFi Enterprise con CAPsMAN e Windows NPS
www.youtube.com/watch?v=RXkoAimlcM8
- Slide MikroTik - WiFi Enterprise con CAPsMAN e Windows NPS
https://mum.mikrotik.com/presentations/EU18/presentation_5159_1523293520.pdf
- Manuale per lo scripting su dispositivi MikroTik
<https://wiki.mikrotik.com/wiki/Manual:Scripting>
- Documentazione FreeRADIUS
<https://freeradius.org/documentation>

- Guida a Systemd
<https://wiki.archlinux.org/index.php/Systemd>
- Guida all'utilizzo di sendmail
<https://secure.php.net/manual/en/function.mail.php>
- Introduzione e guida a Directory Lister
<https://www.directorylister.com>