PROPOSTA DI SOLUZIONE PER LA SECONDA PROVA DI MATURITÀ 2024

TRACCIA: Sistemi e reti

ARGOMENTO: Infrastruttura di rete e sicurezza informatica applicate a contesti specifici.

Testo:

PRIMA PARTE

Punto 1: Descrizione dell'infrastruttura di rete in fibra pre-esistente ed evoluzione

L'infrastruttura di rete in fibra ottica della Regione si estende su una vasta area, collegando attualmente enti locali, scuole e strutture sanitarie pubbliche attraverso sottoreti IP della classe 10.0.0.0/8. All'interno di questa architettura, le sottoreti sono organizzate gerarchicamente per distinguere le diverse tipologie di utenti e di servizi erogati. Integrato nel sistema è presente anche un data-center regionale che raccoglie tutti i dati sanitari dei cittadini residenti in tale regione, inclusi i dati provenienti dal Fascicolo Sanitario Elettronico (FSE).

Questo è un semplice schema della rete attuale:

Enti Locali ---------- Router Regionale ---- Strutture Sanitarie Pubbliche
|
Data-center
Regionale

Con l'introduzione del servizio anche per le strutture sanitarie private convenzionate, che verranno identificate nella sottorete 10.100.0.0/16, l'evoluzione della rete prevede l'ampliamento dell'infrastruttura esistente. Il nuovo segmento sarà dedicato esclusivamente alla connettività delle strutture sanitarie private convenzionate con il data-center regionale, senza fornire loro accesso diretto a Internet per preservare la sicurezza e il controllo dell'accesso ai dati sensibili.

Soluzione a cura di
Lorenzo Pollicino
Insegnante di Sistemi e reti su Ripetizioni.it

La distribuzione degli indirizzi IP nella nuova configurazione sarà di questa tipologia:

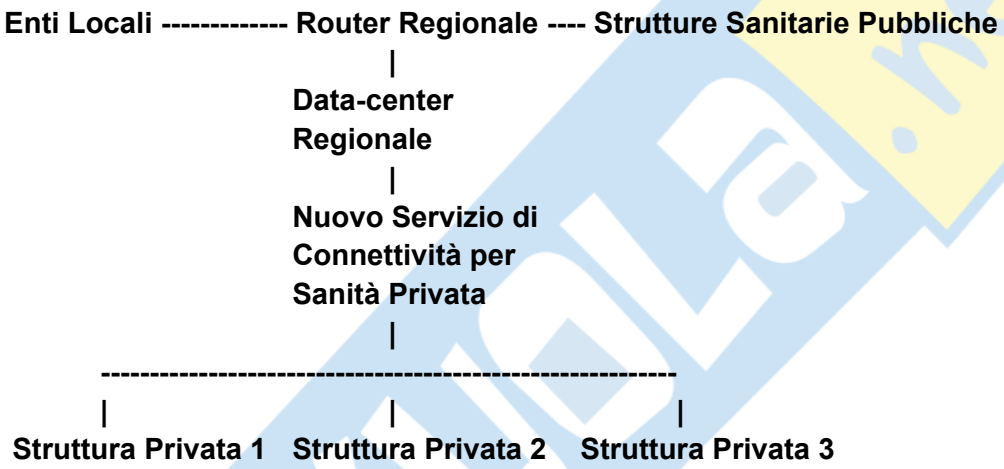
10.0.0.0/8 (Rete regionale in fibra ottica)

10.10.0.0/16 (Enti locali e scuole)

10.20.0.0/16 (Strutture sanitarie pubbliche)

10.100.0.0/16 (Strutture sanitarie private convenzionate)

Questo è un semplice schema della rete dopo l'evoluzione:



Punto 2: Dispositivi forniti alle strutture sanitarie private convenzionate

I dispositivi hardware forniti alle strutture private convenzionate, necessari per connettersi alla nuova rete, saranno principalmente di tre tipologie:

1. I primi dispositivi sono i **router**, scelti in classe enterprise, equipaggiati con un minimo di 4 porte gigabit Ethernet (LAN) e 2 porte WAN per la connessione alla rete regionale. E' necessario che i router abbiano il supporto alle tecnologie VLAN (Virtual Local Area Network) e QoS (Quality of Service), rispettivamente per il supporto delle reti logiche e qualità nella trasmissione dei pacchetti.

2. I secondi dispositivi sono i **firewall** hardware dedicati. Devono avere un minimo di 4

porte gigabit Ethernet ed essere muniti di importanti funzionalità quali il controllo degli accessi, VPN e IDS/IPS. I firewall sono dispositivi progettati per proteggere le reti controllando il traffico in entrata e in uscita. Sono ottimizzati per fornire prestazioni elevate e sicurezza avanzata, essendo dedicati esclusivamente a tale scopo.

3. Infine vengono forniti gli **switch** con gigabit gestito, muniti di almeno 24 porte gigabit Ethernet. Si tratta di dispositivi progettati per facilitare la comunicazione tra device collegati alla stessa rete locale (LAN). La loro principale caratteristica è la capacità di gestire e indirizzare il traffico di rete in modo più sofisticato rispetto agli switch non gestiti.

La configurazione software avviene in modalità remota da parte di tecnici specializzati e utilizzando protocolli sicuri (SSH, HTTPS). Viene, inoltre, configurata la rete VLAN per segmentare il traffico interno ed esterno. Infine si procede con l'implementazione delle regole di sicurezza agendo su firewall e si implementa il QoS per garantire che i servizi critici abbiano priorità sulle risorse di rete, assicurando che applicazioni sensibili come le chiamate vocali o il videoconferenza abbiano un'esperienza fluida e senza interruzioni, anche in condizioni di congestione della rete.

Punto 3: Configurazione della LAN interna delle strutture sanitarie private convenzionate

La configurazione degli apparati esistenti prevede in un primo momento l'intervento sui router e sugli switch e successivamente sui dispositivi di rete quali PC, stampanti e dispositivi di telemedicina.

Per quanto riguarda i router, ogni struttura riceverà un router pre-configurato dalla società regionale che gestisce l'infrastruttura di rete in fibra ottica. Sarà il punto principale di accesso alla rete regionale e sarà configurato per stabilire una connessione VPN IPsec o SSL/TLS con il data-center regionale. Questo permetterà di trasmettere in modo sicuro i dati del fascicolo sanitario elettronico tra la struttura e il data-center, proteggendo la riservatezza delle informazioni sanitarie.

Gli switch invece dovranno essere configurati per supportare la VLAN 100 e per garantire la separazione del traffico. Questo implica la creazione di VLAN tagging sulle porte dei dispositivi che devono accedere alla rete regionale.

Infine gli apparati interni (PC, server, dispositivi medici) dovranno essere configurati con indirizzi IP validi appartenenti alla sottorete 10.100.0.0/16. Questi indirizzi IP saranno

assegnati manualmente o tramite DHCP, a seconda delle politiche di gestione della rete adottate dall'amministrazione della struttura.

Punto 4: Sicurezza dei dati trattati nel fascicolo sanitario elettronico

I dati sensibili, inclusi nel fascicolo sanitario elettronico, devono essere archiviati in modo sicuro sia in locale che tramite un servizio cloud regionale. Tutti i dati, in entrambi i casi, verranno crittografati con sistemi robusti al fine di proteggere i dati sia in fase di archiviazione che durante le operazioni di trasmissione. La crittografia impiegata sarà di tipo AES (Advanced Encryption Standard), DES (Data Encryption Standard) o la più complessa RSA (asimmetrica) e garantirà che solo le persone autorizzate potranno accedere ed interpretare i dati utilizzando le chiavi di sicurezza. Verranno implementati anche sistemi di "disaster recovery" per garantire la continuità operativa in caso di incidenti o catastrofi naturali. I backup dei dati saranno verificati periodicamente tramite test di ripristino per garantire che siano sempre ripristinabili.

Per la trasmissione dei dati dal data-center regionale alle strutture sanitarie private convenzionate e viceversa, è stata, come visto in precedenza, implementata una VPN (Virtual Private Network) sicura. La VPN sfrutterà protocolli crittografici come IPsec (Internet Protocol Security) o SSL/TLS (Secure Sockets Layer/Transport Layer Security) per garantire che tutte le comunicazioni tra la rete regionale e le strutture sanitarie private convenzionate siano crittografate e protette da accessi non autorizzati.

E' opportuno formare adeguatamente il personale delle strutture sulla sicurezza informatica dei dati e sui rischi legati alla possibilità di attacchi cibernetici volti al furto di dati personali dei clienti. Tale formazione è fondamentale per prevenire attacchi di ingegneria sociale che spesso portano l'operatore ad essere vittima di phishing causando un grave danno all'azienda e ai clienti coinvolti.

Soluzione a cura di
Lorenzo Pollicino
Insegnante di Sistemi e reti su Ripetizioni.it

SECONDA PARTE

I. Strategie in caso di malfunzionamenti della connessione e dell'archiviazione dati

In caso di malfunzionamenti durante il trasferimento dei dati o durante il caricamento nei sistemi di archiviazione, è essenziale adottare strategie di mitigazione per evitare perdite di informazioni. Tra le più importanti strategie troviamo l'implementazione di un sistema automatico di backup completi e incrementali dei dati critici su sistemi di archiviazione di diversa natura e dislocati graficamente. Tale accorgimento fa sì che in caso di guasto del sistema primario o di perdita accidentale di dati, sia possibile ripristinare le informazioni senza importanti perdite.

Un altro accorgimento potrebbe essere quello di configurare sistemi di failover automatico su più connessioni di rete. Ad esempio, utilizzare router e switch opportunamente configurati per commutare automaticamente su connessioni di backup (come linee DSL o connessioni rete 4G/5G) nel caso in cui la connessione principale alla fibra ottica regionale fallisca. Il passaggio ad una rete alternativa assicura che le strutture sanitarie possano continuare ad essere operative anche durante interruzioni di rete.

Infine sarebbe opportuno implementare strumenti di monitoraggio avanzato delle reti (automatico o gestito da operatori specializzati in locale o da remoto) che rilevino tempestivamente anomalie di prestazioni e malfunzionamenti nei dispositivi e nelle reti. La presenza di tale servizio consente interventi rapidi per risolvere i problemi prima che questi possano causare interruzioni significative.

II. Autenticazione qualificata per consultazione web del fascicolo sanitario elettronico

Per consentire ai cittadini di consultare in modo sicuro il proprio fascicolo sanitario elettronico via web, è necessario implementare un sistema di autenticazione qualificata a più fattori.

L'autenticazione a più fattori (MFA) consiste nell'utilizzare un sistema di autenticazione che richieda più elementi per verificare l'identità corretta dell'utente. Questi elementi possono includere:

- Una password robusta composta da una combinazione di lettere, numeri e caratteri speciali.

Soluzione a cura di
Lorenzo Pollicino
Insegnante di Sistemi e reti su Ripetizioni.it

- Un token OTP (One-Time Password), che consiste nell'invio all'utente di un codice temporaneo via SMS, app mobile o e-mail.
- Autorizzazione biometria, rappresentata dalla verifica tramite impronte digitali, iride, riconoscimento facciale o altri dati biometrici.
- Lo SPID (Sistema Pubblico di Identità Digitale), ovvero un sistema di identità digitale che consente ai cittadini di accedere in modo sicuro ai servizi online della pubblica amministrazione e di altri enti privati convenzionati.

III. Configurazione del router per una piccola azienda con server locale accessibile da Internet

Per consentire l'accesso al server web locale tramite protocolli HTTP, HTTPS e la gestione remota via SSH attraverso un router con un singolo indirizzo IP pubblico statico, la configurazione richiede una serie di implementazioni. Prima di tutto è necessario configurare il NAT (Network Address Translation) per instradare il traffico proveniente dall'indirizzo IP pubblico statico assegnato al router verso il server web locale. Questo permette al server di essere accessibile pubblicamente su Internet attraverso HTTP e HTTPS. Successivamente si può procedere con l'abilitazione del protocollo SSH sul router e la configurazione delle regole di accesso per consentire connessioni SSH sicure al server web locale. Questo sistema consente alla rete interna di gestire e monitorare il server in modo sicuro e da remoto, senza esporre il server a rischi di sicurezza. E' opportuno anche implementare regole di firewall sul router per limitare l'accesso solo ai servizi necessari (HTTP, HTTPS, SSH) e agli indirizzi IP autorizzati.

Un esempio di comandi utilizzabili per la configurazione di quanto descritto in precedenza sono:

 # Configurazione del NAT per HTTP
ip nat inside source static tcp <indirizzo locale server HTTP> 80 <indirizzo IP pubblico> 80

 # Configurazione del NAT per HTTPS
ip nat inside source static tcp <indirizzo locale server HTTPS> 443 <indirizzo IP pubblico> 443

 # Abilitazione del remote management via SSH
line vty 0 4
transport input ssh

Soluzione a cura di
Lorenzo Pollicino
Insegnante di Sistemi e reti su Ripetizioni.it

IV. Individuazione delle cause di impossibilità di navigare su Internet in un'azienda

Per individuare le possibili cause del problema segnalato dall'utente riguardo all'impossibilità di "navigare su Internet", il tecnico di help-desk può seguire una serie di passaggi strutturati utilizzando gli strumenti appropriati.

Innanzi tutto può verificare con l'utente se il problema si manifesta su tutti i dispositivi collegati alla rete o solo su un dispositivo specifico in modo da comprendere se il problema è limitato a un singolo dispositivo o se coinvolge l'intera rete. Successivamente può assicurarsi che tutti i cavi di rete siano correttamente collegati sia sul lato dell'utente che sul lato del router o switch di rete ed assicurarsi che tutti i dispositivi (router, switch, access point) siano accesi e funzionanti. Se tutto è connesso e acceso, il tecnico può proseguire la sua indagine accedendo al computer dell'utente e verificando se il dispositivo ha un indirizzo IP valido assegnato dal server DHCP o correggerlo se è configurato manualmente; assicurarsi che il gateway predefinito sia correttamente impostato per l'accesso a Internet; controllare le impostazioni DNS per assicurarsi che siano corrette e che il server DNS sia raggiungibile.

L'operatore può procedere con alcuni test tramite prompt dei comandi, ad esempio la verifica del ping verso il gateway predefinito per verificare la connettività locale:

ping <indirizzo_gateway>

E successivamente la verifica del ping verso un sito web esterno per verificare la connettività Internet:

ping www.google.com

Se il ping verso il sito esterno ha successo, significa che il problema potrebbe essere legato al browser o alle impostazioni DNS. Se fallisce, potrebbe esserci un problema con la connessione Internet del provider.

Altre verifiche che il tecnico può eseguire riguardano l'apertura di diversi siti web con protocolli diversi (HTTP o HTTPS); testare browser diversi (Chrome, Mozilla, ecc..); verificare la larghezza di banda per identificare se ci sono problemi di congestione o un utilizzo anomalo delle risorse da parte di qualche dispositivo o applicazione; assicurarsi che non ci siano regole del firewall che possano bloccare il traffico verso Internet. Verificare anche che il router abbia le configurazioni corrette per instradare il traffico Internet correttamente.

Soluzione a cura di
Lorenzo Pollicino
Insegnante di Sistemi e reti su Ripetizioni.it

Se tutte le verifiche precedenti non hanno risolto il problema sarà necessario contattare il fornitore del servizio internet (ISP) per segnalare i problemi di connessione alla rete.

Soluzione a cura di
Lorenzo Pollicino
Insegnante di Sistemi e reti su Ripetizioni.it