Relazione a cura di Varesio Massimo

PROVA TECNICO OPERATIVA B

TECNICO SISTEMISTA DI RETI

Scenario

L'azienda Gamajo s.r.l. ha deciso di incrementare il proprio livello di sicurezza adottando un Firewall aziendale. Il tema di esame richiede di configurare il Firewall secondo le regole indicate e d di implementare un DMZ dove sarà posizionato il server WEB aziendale. La presente relazione sarà struttura in ottica di continuità con la precedente prova operativa A; pertanto, lo schema di rete e alcune indicazioni sono da seguire in riferimento alla relazione della prova A.

Firewall e DMZ

Un Firewall è un dispositivo preposto alla sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare il traffico di rete o specifici eventi. Per dispositivo si intende un elemento hardware o un'applicazione software. I Firewall informatici controllano il traffico di dati in entrambe le direzioni per impedire l'entrata o l'uscita di connessioni pericolose per il sistema. Dal punto di vista del funzionamento, un Firewall è una specie di filtro che controlla il traffico di dati e blocca le trasmissioni pericolose o indesiderate in base a una serie di regole specifiche. La maggior parte dei Firewall dispone di norme standard a cui l'utente finale può aggiungere altre personalizzate, in base alle proprie necessità. Esistono vari tipi di Firewall, ognuno dei quali analizza determinate caratteristiche delle trasmissioni di dati. Il Firewall si interpone tra la rete esterna, che comprende Internet, e la rete interna dell'azienda, di casa o semplicemente il computer dell'utente finale. Da un punto di vista teorico, la rete interna è considerata conosciuta, sicura, attendibile e protetta, mentre quella esterna è la presunta fonte di potenziali minacce, in quanto nel complesso è sconosciuta, insicura e non attendibile.

I Firewall continuano a rappresentare un componente importante della sicurezza aziendale e negli anni hanno continuato ad evolvere per tenere conto delle nuove minacce.

Il Firewall aziendale andrà quindi ad implementare policy di sicurezza attraverso le quali verrà definito il traffico che può transitare da una rete all'altra e quello che deve essere bloccato, in quanto rischioso per la

rete o le reti che devono essere protette. Le policy di sicurezza vengono generalmente implementate mediante le cosiddette Access Control List (ACL), ovvero liste ordinate di condizioni (ad esempio su IP e protocolli) a cui è associato un target (es. permit/deny). Ogni pacchetto viene confrontato in ordine con tutte le condizioni e viene inviato a destinazione o scartato a seconda di cosa prevede il target della prima ACL per la quale la condizione è verificata. Se nessuna condizione viene soddisfatta il pacchetto viene scartato o inviato a destinazione secondo quanto previsto dal target di default impostato sul Firewall.

In riferimento alla pila ISO/OSI, il Firewall opera a livello Applicativo o, più precisamente, ci consente di impostare regole dal terzo livello in avanti (dal livello 3 Network fino al livello 7 Applicazione).

Una prima valutazione che occorre fare in merito all'utilizzo di Firewall nel contesto aziendale è la tipologia di Firewall del quale ci si vuole dotare e il suo posizionamento all'interno della rete aziendale, visto che i Firewall devono essere attraversati dal traffico che deve essere controllato. Occorre quindi conoscere:

- la struttura della rete aziendale;
- quale tipologia di traffico la attraversa;
- la necessità di utilizzare una o più DMZ o di creare zone segregate;
- dove sono i dati e i sistemi che devono essere protetti;
- quali sono le minacce ed eventuali pattern di attacco.

In merito al posizionamento, la scelta più usuale è quella del Firewall perimetrale, che costituisce il posizionamento tradizionale del Firewall aziendale. Il Firewall viene posizionato sul perimetro della rete aziendale con la finalità di proteggere la rete aziendale dagli attacchi provenienti dall'esterno. Sebbene la presenza di un Firewall perimetrale sia sicuramente necessaria, è anche vero che non può essere considerata sufficiente. Il fatto che sempre più servizi aziendali debbano essere esposti su Internet fa nascere l'esigenza di una DMZ, una rete ove vengono posizionati i sistemi esposti su Internet e isolata il più possibile dalla rete interna, in modo che eventuali compromissioni di tali sistemi non abbiano ricadute immediate sui sistemi interni.

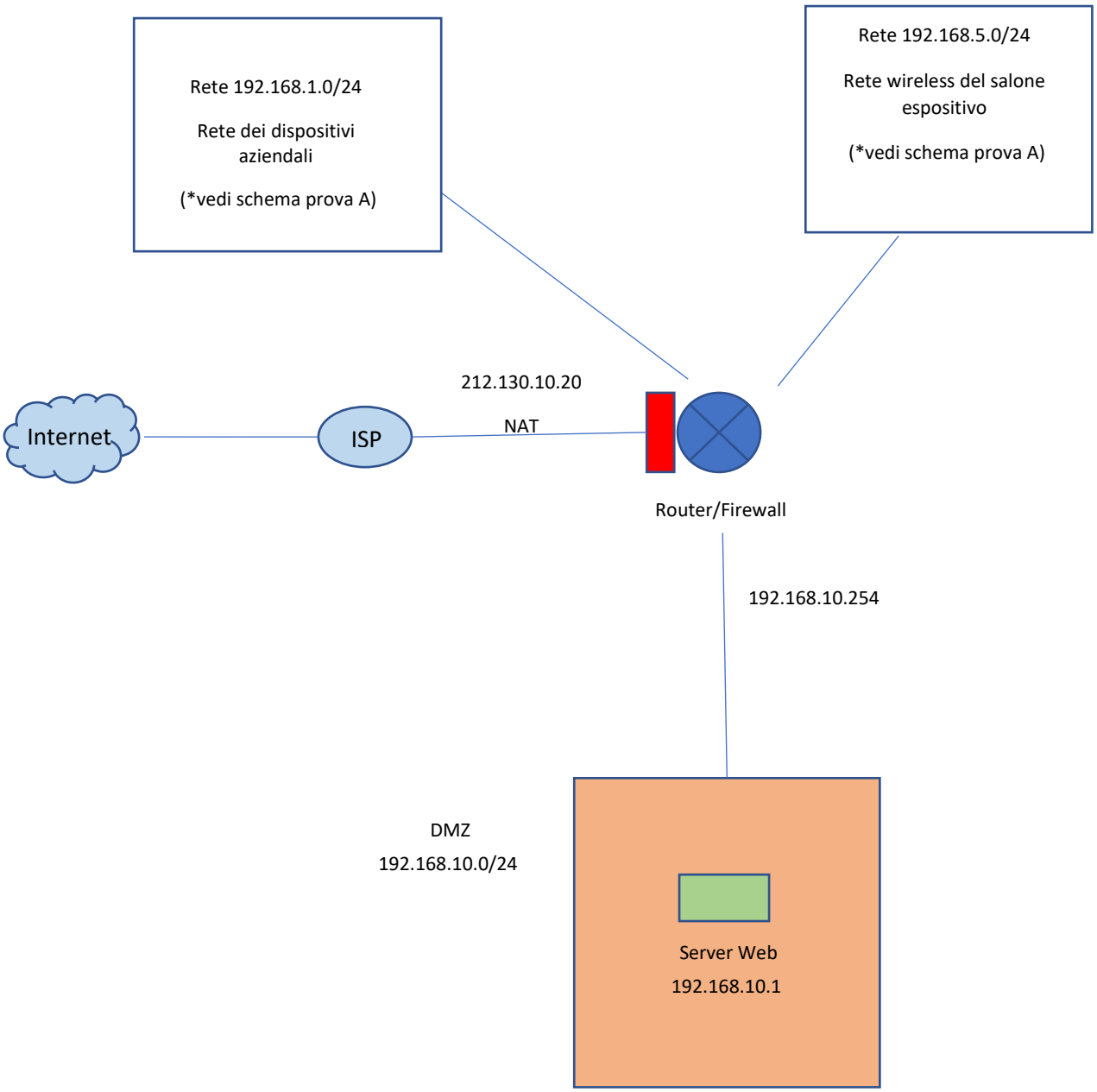
La DMZ è una forma di segmentazione, spesso ottenuta attraverso il Firewall perimetrale stesso. Nello specifico, la DMZ è un'area della rete interposta tra la rete esterna e la rete interna, usata per consentire l'accesso dalla rete pubblica esterna a server o altri componenti, ad esempio server mail e server WEB, in modo da non compromettere la rete interna da proteggere. Si possono utilizzare uno o più Firewall per isolare le DMZ, che generalmente agiscono con sistemi di tipo packet filter, e consentono la comunicazione da parte delle macchine nella rete interna tramite il servizio NAT.

Il caso dell'azienda Gamajo s.r.l.

Come richiesto dal tema di esame, nella zona DMZ dobbiamo prevedere il server WEB essenziale per l'erogazione dei servizi web dell'azienda accessibili su Internet. L'indirizzo del server sarà mappato in modo statico, grazie all'apparato di sicurezza principale della rete aziendale. Bisogna ricordare che per essere davvero accessibili questi servizi, il server erogante dovrà avere oltre ad un IP fisso anche la registrazione di un dominio riservato all'azienda. Questo andrà fatto su tramite un'apposita autorità di registrazione/ISP in grado di garantire la registrazione su qualche server DNS della rete. Come già predisposto nella prova A, è opportuno prevedere anche un servizio DNS interno che preveda la copertura (corrispondenza nome/IP) delle macchine della rete, o di parte di esse. Tale funzionalità è stata prevista nello schema con una apposita macchina server che combina le funzionalità DHCP e quelle di un servizio DNS interno alla LAN.

Il complesso di dispositivi che si trova a contatto con Internet, sarà costituito da un Router con funzioni di Firewall, ossia un apparato che permette ai computer della rete di uscire su Internet in modo controllato ed isolato rispetto alla rete stessa. Tale apparato specializzato è in grado di differenziare, sulle proprie uscite, una zona meno protetta (DMZ) ed una con più alta protezione. Andranno imposte delle opportune ACL che lascino aperte non tutte le porte (e gli IP) indiscriminatamente, ma solo quelle(/i) relative(/i) ai due servizi attivi ed erogati, nel nostro caso i servizi web dell'azienda. Questa opera di selezione consente di chiudere molti possibili punti di attacco, lasciando pochi e ben definiti canali tramite i quali si possa accedere a DMZ da Internet e facendo aumentare la sicurezza anche dei sistemi nella DMZ.

Schema tecnico-grafico



Configurazione del Firewall aziendale

Il Firewall lavora su delle regole impostate che vengono eseguite in base all'ordine (gerarchico) e a cui corrisponde un'azione ad esempio:

- ACCEPT: accetta il passaggio di pacchetti da e verso le sorgenti/destinazioni presenti nella regola;
- BLOCK o DROP: scarta il pacchetto in modo silente senza generare messaggi di risposta;

- REJECT: rifiuta il pacchetto e risponde con un pacchetto ICMP.

I termini utilizzati per l'inserimento delle regole possono variare a seconda della configurazione prevista da Vendor del dispositivo Firewall, ma il significato di base rimane il medesimo.

Di seguito verrà realizzata una tabella contenente uno schema semplificato e simulato per l'inserimento delle regole richieste dal tema di esame:

1. il Firewall dovrà consentire il solo traffico HTTP, HTTPS e FTP da e verso la rete interna;
2. il Firewall dovrà redirigere il traffico esterno diretto alla porta HTTP sulla corrispondente porta del server WEB;
3. il Firewall dovrà permettere l'accesso tramite protocollo RDP su una porta non convenzionale al PC del sistemista.

N° ACL	**Nome**	**Direzione**	**Traffico**	**Protocollo**	**Origine**	**Porta origine**	**Destinazione**	**Porta destinazione**	**Azione**
1	consenti-http-a-internet	In uscita	IP pubblico o traffico Internet	HTTP	Qualsiasi (inteso come ogni PC dei dip. aziendali)	Qualsiasi	Qualsiasi	80	Consenti
2	consenti-http-da-internet	In entrata	IP pubblico o traffico Internet	HTTP	Qualsiasi	Qualsiasi	192.168.10.1 (IP server WEB)	80	Consenti
3	consenti-https-a-internet	In uscita	IP pubblico o traffico Internet	HTTPS	Qualsiasi (inteso come ogni PC dei dip. aziendali)	Qualsiasi	Qualsiasi	443	Consenti
4	consenti-https-da-internet	In entrata	IP pubblico o traffico Internet	HTTPS	Qualsiasi	Qualsiasi	192.168.10.1 (IP server WEB)	443	Consenti
5	consenti-ftp-a-internet	In uscita	IP pubblico o traffico Internet	FTP	Qualsiasi (inteso come ogni PC dei dip. aziendali)	Qualsiasi	Qualsiasi	20/21	Consenti
6	consenti-ftp-da-internet	In entrata	IP pubblico o traffico Internet	FTP	Qualsiasi	Qualsiasi	192.168.10.1 (IP server WEB)	20/21	Consenti
7	consenti-da-rdp	In entrata	IP pubblico o traffico Internet	RDP	Qualsiasi	Qualsiasi	192.168.1.3 (IP specifico del PC del sistemista)	5555 (decisa in modo casuale)	Consenti
8	nega-tutto-da-internet	In entrata	IP pubblico o traffico Internet	Tutti i protocolli	Qualsiasi	Qualsiasi	Qualsiasi	Qualsiasi	Rifiuta

Precisazioni:

- RDP (Remote Desktop Protocol) è un protocollo di rete proprietario sviluppato da Microsoft, che permette la connessione remota da un computer a un altro utilizzando l'interfaccia grafica (GUI) di Windows, usando di

default la porta TCP e UDP 3389. Nella tabella è stata indicata la porta 5555 (scelta in modo casuale) al posto della 3389;

- la regola 8 è stata pensata per rifiutare tutto il traffico proveniente da Internet che non sia autorizzato dalle regole superiori. Per completezza, si potrà definire la priorità sulle altre regole rispetto alla 8;
- per le indicazioni della tabella si sono utilizzate le porte standard anche dette "Well know port";
- rispetto a quanto indicato in tabella, alcune delle regole potrebbero dover essere impostate inserendo quale protocollo il TCP/UDP del livello trasporto, principale responsabile della trasmissione dei pacchetti;
- i termini utilizzati in tabella sono frutto di una simulazione e non corrispondono necessariamente a termini relativi ad un Firewall reale.

IPS e IDS

Il miglior modo per proteggere una rete o un singolo computer sta nel riconoscere e respingere in maniera preventiva gli attacchi, ancora prima che questi possano causare danni. Molti si affidano per questo ai cosiddetti Intrusion Detection System (IDS) o ai più versatili Intrusion Prevention System (IPS). Entrambi i sistemi possono essere implementati nelle funzionalità di Switch intelligenti e Firewall di fascia medio-alta. Un Instrusion Detection System (IDS), che in italiano è traducibile con sistema di rilevamento delle intrusioni, serve a individuare in anticipo attacchi verso un computer o una rete. I software IDS possono essere installati sia direttamente sul sistema che si vuole controllare, sia su un dispositivo separato. Gli Intrusion Detection System controllano ed analizzano tutte le attività di rete, al fine di scovare un traffico dati insolito e quindi, in tal caso, informare l'utente interessato. In questo modo l'utente ha la possibilità di reagire ai tentativi di accesso da parte dell'intruso e bloccare questi attacchi sul nascere. L'Intrusion Prevention System (IPS), che può essere liberamente tradotto in italiano con sistema di prevenzione delle intrusioni, come suggerisce il nome, va oltre all'Intrusion Detection System: dopo aver appurato la possibilità di un attacco, questo tipo di sistema non si limita ad informare l'amministratore, ma attiva immediatamente delle misure di sicurezza adeguate. In questo modo evitano che passi un intervallo di tempo troppo lungo tra il rilevamento di un intruso e l'attuazione di azioni volte a fermarlo, come può invece capitare con i programmi IDS. Per quanto riguarda i metodi di analisi dei dati utilizzati dai due meccanismi di difesa della rete, non vi è una grande differenza. Oggi come oggi un IPS così come un IDS ricorrono agli stessi sensori, basati su host e su rete, allo scopo di registrare e classificare i dati del sistema e i pacchetti di rete.

VPN per accesso da remoto

Nel caso in cui alcuni dipendenti dell'azienda avessero la necessità di connettersi da remoto verso la LAN interna, occorrerà adottare un sistema sicuro, ossia un collegamento tramite VPN (Virtual Private Network).

Una VPN consente di creare una rete privata virtuale che garantisce privacy, anonimato e sicurezza dei dati attraverso un canale di comunicazione riservato tra dispositivi che non necessariamente devono essere collegati alla stessa LAN. Una VPN o Virtual Private Network (Rete virtuale privata) crea una connessione di rete privata tra dispositivi su Internet. Le VPN sono utilizzate per trasmettere dati sulle reti pubbliche in modo anonimo e sicuro. Funzionano camuffando gli indirizzi IP dell'utente e crittografando i dati in modo che non possano essere letti da chi non è autorizzato a riceverli. Una connessione VPN reindirizza i pacchetti di dati dalla macchina locale a un altro server remoto prima di inviarli a terze parti su Internet. Tra i principi chiave dietro alla tecnologia VPN possiamo trovare:

- protocollo di tunneling: una rete privata virtuale crea un tunnel dati sicuro tra il tuo computer locale e un altro server VPN in una posizione a distanza. Quando ci si connette, questo server VPN diventa la fonte di tutti i dati. Il fornitore di servizi Internet (ISP) e altre terze parti non possono più visualizzare i contenuti del traffico criptato.
- crittografia: i protocolli VPN come l'IPsec codificano i dati prima di inviarli attraverso il tunnel dati. L'IPsec è una suite di protocolli che si prefigge di ottenere connessioni sicure a livello di protocollo IP mediante l'autenticazione e la crittografia dei singoli pacchetti IP del flusso dei dati. Il servizio VPN agisce come filtro, rendendo i dati criptati illeggibili da un lato e decodificandoli dall'altro lato: questo impedisce l'utilizzo improprio dei dati personali, anche se la connessione Internet dovesse essere compromessa. Il traffico di rete non è più vulnerabile agli attacchi e la connessione Internet è sicura.

Le aziende sfruttano spesso le VPN in quanto costituiscono un modo conveniente, veloce e sicuro per far connettere gli utenti da remoto alla rete aziendale.

Best practices in materia di sicurezza

La Governance della sicurezza del sistema informativo aziendale comporta:

- definizione e attuazione di politiche per la sicurezza;
- definizione e attuazione di processi gestionali controllati;
- raccolta tempestiva di informazioni e dati per poter controllare e misurare i servizi;
- controllo e misura di eventuali scostamenti dai requisiti dettati da normative e regolamenti (GDPR).

Sarà senz'altro opportuno gestire il dominio aziendale mediante un sistema AAA, introducendo sul sistema informativo delle componenti infrastrutturali che offrono servizi di autenticazione, autorizzazione e accounting degli utenti delle applicazioni:

- AUTENTICAZIONE: meccanismi per accertare l'identità dell'utente;
- AUTORIZZAZIONE: meccanismi di verifica e attuazione delle regole di autorizzazione assegnate ad un utente per l'esecuzione di una determinata funzionalità applicativa o per l'accesso ad un dato o tipo di dato;
- ACCOUNTING: meccanismi di responsabilizzazione dell'utente, anche attraverso il tracciamento delle operazioni svolte sui dati mediante le applicazioni o gli altri strumenti resi disponibili sul sistema informativo.

Per garantire una corretta politica di autorizzazione degli utenti è opportuno definire un insieme di ruoli applicativi che sia possibile attribuire agli utenti. Ciascun ruolo prevede un insieme di autorizzazioni che saranno così attribuite a tutti gli utenti a cui verrà assegnato un determinato ruolo (come fatto nella prova A). Si costruisce un profilo dell'utente del sistema informativo basato sui ruoli (e quindi sulle autorizzazioni) che si assegnano all'utente; assegnare o rimuovere un ruolo ad un utente significa assegnare o rimuovere un insieme di autorizzazioni allo stesso utente in un'organizzazione strutturata, come nel caso dell'azienda Gamajo s.r.l. proposta nel tema di esame.

Procedure per controlli di sicurezza:

- **vulnerabily assessment**: verifica la presenza di vulnerabilità note e della corretta configurazione dei sistemi (es.: disabilitazione di porte TCP e di servizi secondo quanto previsto dalle politiche di sicurezza aziendali), è un'attività svolta mediante appositi strumenti che eseguono la scansione automatica delle porte di rete dei diversi apparati alla ricerca dei servizi attivi ed eseguono la

verifica della configurazione (software installato, versioni del software, applicazione di patch di sicurezza, ecc.);

- **penetration test**: attraverso un'attività manuale o automatizzata con strumenti software automatici, si prova a violare la sicurezza di un'applicazione o di un sistema, verificando la presenza di errori che consentono accessi non autorizzati e modifica o acquisizione di dati riservati.

Da ultimo, ma non per importanza, ai fini della sicurezza dei dati aziendali sarà necessario implementare dei meccanismi di Disaster Recovery che permettano il ripristino dell'infrastruttura IT in caso di guasti, catastrofi naturali o attacchi informatici. Il modo più comune per implementare tali politiche di sicurezza consiste nell'effettuare processi di Backup a intervalli regolari. Con il termine Backup, nella sicurezza informatica, si indica un processo per la messa in sicurezza delle informazioni di un sistema informatico attraverso la creazione di ridondanza delle informazioni stesse (una o più copie di riserva dei dati), da utilizzare come recupero (ripristino) dei dati stessi in caso di eventi malevoli accidentali o intenzionali o semplice manutenzione del sistema. Un Backup può, come già detto, anche risultare utile per proteggersi da attacchi informatici. Si tratta di un processo fondamentali nell'ottica della Business Continuity di qualsiasi realtà aziendale.