ESERCIZIO DEL 15/04/2024 STEFANO CESARONI

I FIREWALL SONO DEI DISPOSITIVI HARDWARE O SOFTWARE CON LO SCOPO DI PROTEGGERE LA RETE DALLE MINACCIE ESTERNE. REGOLA IL FLUSSO DI DATI CONSENTENDO O BLOCCANDO I DATI E POSSONO ESSERE PERIMETRALI(A CAVALLO TRA WAN E LAN) E NON PERIMETRALI.

ESISTONO 3 TIPI DI FIREWALL:STATICO, DINAMICO E PER CONTENUTO.

IL FIREWALL STATICO CONFRONTA TUTTI GLI INDIRIZZI IP CHE VOGLIONO ACCEDERE ALLA RETE. GRAZIE AD UNA LISTA, DETTA ACL, VA A CONFRONTARE DALL’ALTO VERSO IL BASSO LA TABELLA DEGLI INDIRIZZI IP IN CERCA DI UN RISCONTRO. QUESTA ACL VIENE SCRITTA MANUALMENTE ED OGGIGIORNO NON VIENE PIU’ UTILIZZATA.

IL FIREWALL DINAMICO BLOCCA TUTTE LE CONNESIONI SE HANNO ORIGINE DALL’ESTERNO VERSO L’INTERNO E CONSENTE LE CONNESIONI DALL’INTERNO VERSO L’ESTERNO. QUEST’ULTIMA AVVIENE GRAZIE ALLA MEMORIA DINAMICA DEL FIREWALL. ESISTE UNA”ZONA” O PORTA DEL FIREWALL CHIAMATA DMZ. ESSA CONSENTE LA CONNESSIONE DI HOST ESTERNI VERSO I SERVER WEB(ESEMPIO SITO DI AMAZON) E SMTP(POSTA ELETTRONICA).PROTEGGE FINO AL 4° LIVELLO DEL MODELLO ISO/OSI

IL FIREWALL PER CONTENUTO E’ UNA PROTEZIONE DEL WEB E CONTROLLA IL CODICE DEI DATI INVIATI DAGLI HOST ESTERNI, SE LO REPUTA MALEVOLO RIFIUTA IL RICEVIMENTO DEI DATI E BLOCCA LA CONNESIONE. UN ESEMPIO E’ IL WAF E VIENE USATO SPESSO USATO IN AZIENDA INSIEME AL FIREWALL DINAMICO.

NEXT GENERATION FIREWALL: FIREWALL DI NUOVA GENERAZIONE CHE PROTEGGE DA TUTTI E 7 I LIVELLI DEL MODELLO ISO/OSI E POSSIEDE PIU’ SERVIZI DI UN FIREWALL TRADIZIONALE(ANTI SPAM, ANTI MALWARE, WAF ECC.)

NELLA CONFIGURAZIONE DI UNA RETE AZIENDALE SI E’ SCELTO DI METTERE 3 FIREWALL:

FIREWALL 1: E’ UN FIREWALL DINAMICO IN QUESTO PIU’ SICURO PERCHE’ BLOCCA TUTTE LE CONNESIONI CHE HANNO ORIGINE DALL’ESTERNO VERSO L’INTERNO PERMETTENDO IL CONTRARIO.QUESTA PRIMA BARRIERA SI TROVA TRA INTERNET E IL ROUTER GATEWAY DELL’AZIENDA. ALL’INTERNO DI QUESTO FIREWALL IMPOSTIAMO UNA DMZ IN MODO TALE DA PERMETTERE LE CONNESIONI DI HOST ESTERNI AI SERVER WEB E SMTP.

FIREWALL 2: E’ UN FIREWALL PER CONTENUTO(WAF), PROTEGGE I SERVER WEB E SMTP. QUESTA SECONDA BARRIERA SI TROVA TRA IL DMZ E I SERVER

FIREWALL 3: SI TROVA TRA SWICH E IL NAS. SPESSO IN AMBITO AZIENDALE SI UTILIZZA L’IDS(UN SOFTWARE CHE NOTIFICA IL RILEVAMENTO DI UN INTRUSIONE)DIMINUISCE LA SICUREZZA MA AUMENTA LA FLESSIBILITA’ IN QUANTO GLI HOST INTERNI ALL’AZIENDA POSSO ACCEDERE AL NAS SENZA PROBLEMI. IN CASO DI ATTACCO SI PREFERISCE L’INTERVENTO UMANO.

