ӘОЖ 004.056

КИБЕРҚАУІПСІЗДІК. FILTERING. FIREWALL

Калешов Ерген Науырызбайұлы
kaleshovergen@gmail.com
«Бағдарламалық қамтамасыз ету» білім бағдарламасының 3 курс студенті
Жоғары инженерлік технологиялық колледжі, Орал қ, Қазақстан Республикасы
Ғылыми жетекшісі, «Информатика» ғылымының магистрі – **Қанибаева Ө.Т.**

Аннотация: Веб-қосымшаның брандмауэрі немесе WAF - бұл құрал бақылау, сүзу және блоктау үшін қауіпсіздік және веб-қосымшадан немесе веб-сайттан шығатын деректер пакеттері. WAF мүмкін хост, желі немесе бұлтты болыңыз және әдетте орналастырылады кері прокси-серверлер және қолданбаның немесе веб-сайттың алдына орналастырылады (немесе бірнеше қолданбалар мен сайттар).

WAF желілік құрылғылар, сервер плагиндері немесе бұлтты қызметтер, әр пакетті тексеру және қолданбалы логиканы талдау сүзу ережелеріне сәйкес деңгей (7 деңгей) күдікті немесе қауіпті трафик.

Кілт сөздер: қауіпсіздік, бақылау, сүзу, құлыптау, кіріс және шығыс деректер пакеті.

Техникалық тұрғыдан алғанда, Firewall-бұл қажетсіз трафикті бұғаттайтын бағдарламалық жасақтама немесе аппараттық-бағдарламалық жасақтама. Бұл ретте брандмауэр арқылы трафикті өткізу немесе бұғаттау әкімші белгілеген параметрлер бойынша жүзеге асырылады.

Мұндай параметрлердің қатарына мыналар жатады:

- Пакеттерді алуға тыйым салынатын немесе рұқсат етілетін IP мекенжайлары. Сондай-ақ IP мекенжай тізімдеріне тыйым салулар мен рұқсаттар қойылады;
- трафикті өткізіп жіберуге тыйым салынатын тізімге енгізілуі мүмкін веб-сайттардың домендік атаулары;
- бұғаттау немесе рұқсат беру белгілі бір қызметтер мен қосымшаларға қол жеткізуді реттейтін порттар;
- ХЭО үшін нақты хаттамалардан трафикті өткізіп жіберуге тыйым салу немесе рұқсат беру үшін арнайы конфигурацияланатын хаттамалар.

Бұл жағдайда параметрлер бөлек немесе белгілі бір комбинацияларда берілуі мүмкін.

Firewall пайдалану компьютерлер мен желілерді қорғаудың бірқатар мәселелерін шешуге мүмкіндік береді:

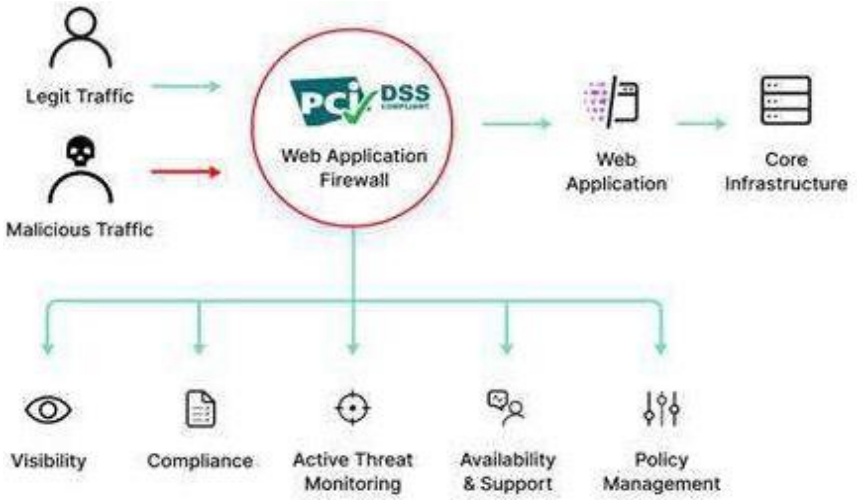
- желі тораптарының әлсіз қорғалған қызметтеріне қол жеткізуді шектеу және бақылау;
- қызметтерге қол жеткізу тәртібін регламенттеу;
- құрылғыларға қол жеткізудің "сыртқы" және "ішкі" әрекеттерін тіркеу және есепке алу;
- желілер мен құрылғылар туралы ақпарат алуға кедергілер орнату арқылы;
- қорғалған желілер туралы жалған ақпарат тарату арқылы.

Алайда, МӘС - тің кемшілігі де бар - оны енгізу кезінде желілік инфрақұрылымды қайта құру қажет болуы мүмкін. Бұған жол бермеу үшін ақпараттық жүйені құрудың алғашқы кезеңдерінде желі топологиясын дұрыс жобалау қажет.

WAF өнімдерді ұсынатын ұйымдардың көбеюі үшін маңызды немесе Интернеттегі қызметтер, соның ішінде мобильді қосымшаларды жасаушылар, әлеуметтік медиа провайдерлері және цифрлық банкирлер. WAF көмектесе алады сіз клиенттердің жазбалары мен деректері сияқты құпия деректерді қорғайсыз және ағып кетудің алдын алыңыз.

Ұйымдар әдетте өздерінің құпиялылығының көп бөлігін сақтайды веб-қосымшалар арқылы қол жеткізуге болатын серверлік мәліметтер базасындағы мәліметтер. Компаниялар

Мобильді қосымшаларды көбірек қолданады және іскерлік өзара әрекеттесуді жеңілдетуге арналған IoT құрылғылары онлайн транзакциялар қолданба деңгейінде орын алады. Зиянкестер көбінесе бұл деректерге қол жеткізу үшін қолданбаларға бағытталған.



Сурет 1. WAF жұмыс процесі.

WAF пайдалану талаптарды орындауға көмектеседі PCI DSS сияқты сәйкестіктер (салалық деректер қауіпсіздігі стандарты кез келген ұйымға қолданылатын төлем карталары), және брандмауэрді орнатуды қажет етеді.

Осылайша, WAF қауіпсіздік моделінің маңызды құрамдас бөлігі болып табылады ұйымдар.

WAF болуы маңызды, бірақ оны басқа шаралармен біріктіру ұсынылады кіруді анықтау жүйелері (IDS), жүйелер сияқты қауіпсіздік кірудің алдын алу (IPS) және дәстүрлі брандмауэрлер терең эшелонды қорғаныс үлгісін алыңыз.

Веб-қосымшалардың брандмауэр түрлері:

WAF енгізудің үш негізгі әдісі бар:

Желілік WAF – әдетте аппараттық құрал, ол орнатылады кідірісті азайту үшін жергілікті. Дегенмен, бұл ең қымбат түрі Физикалық жабдықты сақтау мен техникалық қызмет көрсетуді қажет ететін WAF.

Хостқа негізделген WAF – толығымен біріктірілуі мүмкін қолданбаның бағдарламалық жасақтамасы. Бұл опция желіге қарағанда арзанырақ WAF және теңшелетін, бірақ ол айтарлықтай ресурстарды қажет етеді. Жергілікті сервер, іске асыру қиын және қымбат болуы мүмкін қызмет көрсету. Хостқа негізделген WAF іске қосу үшін қолданылатын машина, көбінесе уақытты қажет ететін және болуы мүмкін нәрсені нығайту және реттеу қажет қымбат.

Бұлтты WAF – қолжетімді, оңай орындалатын шешім, бұл әдетте алдын-ала инвестицияларды қажет етпейді, сонымен бірге пайдаланушылар қызметке ай сайынғы немесе жылдық жазылымды төлейді "Қауіпсіздік Қызмет ретінде". Бұлтты WAF-ты үнемі жаңартып отыруға болады қосымша шығындар және пайдаланушының күш-жігерінсіз. Дегенмен, сіз үшінші тарап ұйымына сенетіндіктен WAF басқару элементтері, бұлтты WAF бар екеніне көз жеткізу маңызды сіздің бизнес ережелеріңізге сәйкес келу үшін жеткілікті теңдеу параметрлері ұйымдар.

WAF функциялары мен мүмкіндіктері

Ксете 1 - Веб-қосымшалардың брандмауэрлері әдетте келесі функциялар мен мүмкіндіктерді ұсынады:

Шабуыл қолтаңбаларының мәліметтер базасы	Шабуыл қолтаңбалары-бұл мүмкін болатын шаблондар сұраныс түрлерін, сервердің аномальды жауаптарын және белгілі зиянды IP мекенжайларын қоса, зиянды трафикті көрсете алады. Бұрын WAF негізінен жаңа немесе белгісіз шабуылдарға қарсы тиімділігі төмен шабуыл шаблондарының мәліметтер базасына сүйенетін.
Жасанды интеллектке негізделген трафик үлгілерін талдау	Жасанды интеллект алгоритмдері мінез-құлықты қолдана отырып, трафиктің әртүрлі түрлеріне арналған негізгі параметрлер, көрсететін ауытқуларды анықтау үшін шабуыл. Бұл шабуылдарды анықтауға мүмкіндік береді, белгілі емес зиянды үлгілер.
Профильдеу қосымшалары	Бұл құрылымды талдауды қамтиды қосымшалар, соның ішінде әдеттегі сұраулар, URL мекенжайлар, мәндер және рұқсат етілген деректер түрлері. Бұл WAF ті анықтауға және бұғаттауға мүмкіндік береді ықтимал зиянды сұраулар.
Орнату	Операторлар қауіпсіздік, мүмкін анықтау қолданылатын ережелер трафикке қосымшалар. Бұл ұйымдарға мүмкіндік береді WAF мінез-құлқын келесіге сәйкес реттеңіз өз қажеттіліктері және алдын алу заңды трафикті бұғаттау.
Механизмдері корреляция	Олар кіріс трафигін талдайды және сұрыптайды ол белгілі шабуыл қолтаңбаларының көмегімен, профильдеу қосымшалар, талдау жасанды интеллект және теңшелетін оны анықтау үшін ережелер блоктау.
Қорғау платформалары DDoS шабуылдары	Сіз бұлтты платформаны біріктіре аласыз, таратылған типті шабуылдардан қорғайды "қызмет көрсетуден бас тарту" (DDoS). Егер WAF DDoS шабуылын анықтайды, ол жібере алады DDoS шабуылынан қорғау платформасына трафик, ол үлкен көлемді өңдей алады және солай.
Жеткізу желілері мазмұны (CDN)	WAF желі шекарасында орналастырылған, сондықтан бұлтты WAF CDN-ді қамтамасыз ете алады веб-сайтты кэштеу және оның уақытын қысқарту жүктеулер. WAF CDN-ді бірнеше рет орналастырады таратылған қатысу нүктелері (PoP) бүкіл әлемде, сондықтан пайдаланушылар ең жақын поптан қызмет көрсетіледі.

WAF технологиясы

WAF сервер жағындағы бағдарламалық плагиндерге ендірілуі мүмкін немесе аппараттық құрылғылар немесе олар ұсынылуы мүмкін трафикті сүзуге арналған қызметтер.

WAF веб-қосымшаларды қорғай алады зиянды немесе бұзылған соңғы нүктелер ретінде жұмыс істейді кері прокси-серверлер (қорғайтын прокси-серверден айырмашылығы зиянды веб-сайттардың пайдаланушылары).

WAF әрқайсысын ұстап алу және зерттеу арқылы қауіпсіздікті қамтамасыз етеді HTTP сұрауы. Заңсыз трафикті әр түрлі көмегімен тексеруге болады құрылғыдан саусақ іздерін алу, құрылғыны талдау сияқты әдістер captcha енгізу және тексеру, егер олар заңсыз болып көрінсе, сіз жасай аласыз бұғаттау.

WAF алдын-ала жүктелген қауіпсіздік ережелеріне ие көптеген белгілі шабуыл үлгілерін анықтап, бұғаттай алады-әдетте оларға веб-қосымшалардың қауіпсіздігінің негізгі осалдықтары кіреді, Open Web Application Security Project (OWASP) қолдайды.

Сонымен қатар, ұйым өзінің ережелерін анықтай алады және өз қосымшасының бизнес-логикасына сәйкес қауіпсіздік саясаты.

WAF орнату және конфигурациялау үшін арнайы білім қажет болуы мүмкін.

WAF оң немесе теріс модельді қолдана алады қауіпсіздік немесе екеуінің тіркесімі:

Позитивті қауіпсіздік моделі-позитивті модель WAF қауіпсіздігі трафикті сүзетін ақ тізімді қамтиды рұқсат етілген элементтер мен әрекеттер тізіміне сәйкес-бәрі жоқ тізімде, бұғатталған. Бұл модельдің артықшылығы-ол мүмкін әзірлеуші күтпеген жаңа немесе белгісіз шабуылдарды блоктаңыз.

Теріс қауіпсіздік моделі-теріс модель тек блоктайтын қара тізімді (немесе тыйым салу тізімін) қамтиды белгілі бір элементтер - тізімде жоқ кез келген нәрсеге рұқсат етіледі. Бұл модель іске асыру оңай, бірақ ол бәрін жоюға кепілдік бере алмайды қауіптер. Ол сондай-ақ ықтимал ұзақ тізімді сақтауды талап етеді зиянды қолтаңбалар. Қауіпсіздік деңгейі санға байланысты енгізілген шектеулер.

Қолданылған әдебиеттер тізімі:

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум // А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019, 432 с.
2. Бабаш А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие // А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2013, 136 с.
3. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие // Е.К. Баранова, А.В. Бабаш. – М.: Риор, 2017, 400 с.
4. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие // Е.К. Баранова, А.В. Бабаш. – М.: Риор, 2017, 476 с.
5. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие // Е.К. Баранова, А.В. Бабаш. – М.: Риор, 2018, 400 с.
6. Баранова Е.К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие // Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. – М.: Риор, 2008, 400 с.
7. Бирюков А.А. Информационная безопасность: защита и нападение // А.А. Бирюков. – М.: ДМК Пресс, 2013, 474 с.
8. Гафнер В.В. Информационная безопасность: Учебное пособие // В.В. Гафнер. – Рн/Д: Феникс, 2010, 324 с.
9. Глинская Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие // Е.В. Глинская, Н.В. Чичварин. – М.: Инфра-М, 2018, 64 с.
10. Глинская Е.В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие // Е.В. Глинская, Н.В. Чичварин. – М.: Инфра-М, 2018, 160 с.
11. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие // Н.В. Гришина. – М.: Форум, 2017, 159 с.
12. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие // Н.В. Гришина. – М.: Форум, 2018, 118 с.

13. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие // Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2010, 384 с.

14. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография // Л.Л. Ефимова, С.А. Кочерга. – М.: Юнити-Дана, 2013, 239 с.

15. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография // Л.Л. Ефимова, С.А. Кочерга. – М.: Юнити, 2013, 239 с.