Дәріс №6: Демилитаризациялық аймақ түсінігі

DMZ - демилитаризацияланған аймақ (demilitarized zone) қысқартылған сөз. Бұл термин желінің толық сенімсіз бөлігіне қатысты қолданылады. DMZ - бұл жүйені негізгі желіден бөлетін желідегі аймақ. Мұндай сегментті құрудың мәні Интернет қолданушылары қатынайтын жүйелерді ұйымның қызметкерлері ғана жұмыс жасайтын жүйелерден бөлу болып табылады. Демилитаризацияланған аймақтарды серіктестермен және басқа сыртқы тараптармен жұмыс кезінде де қолдануға болады.

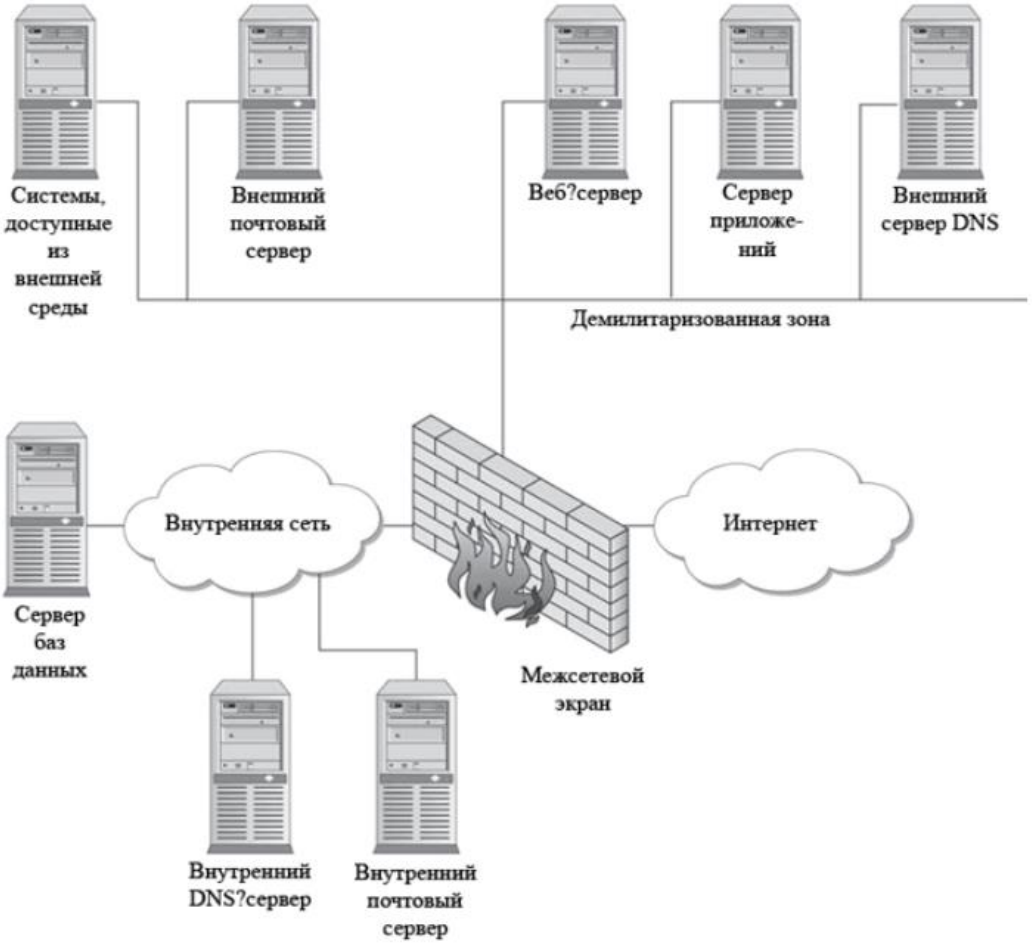
DMZ жартылай қорғалған желілік аймақты енгізу арқылы жасалады. Бұл аймақ әдетте желіаралық экрандар немесе қатаң сүзгілері бар маршрутизаторлар сияқты желілік құрылғылармен бөлінеді. Содан кейін желіні басқару арқылы саясат DMZ-ге қай трафикке кіруге рұқсат етілгенін және DMZ-ден тыс трафикке рұқсат етілгенін анықтайды (1-сурет). Әдетте, сыртқы пайдаланушыларға тікелей байланыс орнатуға болатын кез-келген жүйе САҚТАНДЫРЫЛҒАН АЙМАҚТА болуы керек.

1-сурет. DMZ саясатының негізгі ережелері

Ашық жүйелер сыртқы жүйелерге немесе пайдаланушыларға тікелей қол жеткізу үшін зиянкестердің басты мақсаттары болып табылады және қауіп-қатердің пайда болуына ықтималдылығы бейім. Бұл жүйелер толық сенімге ие бола алмайды, өйткені олар кез-келген уақытта шабуылға ұшырайды. Демек, біз осы жүйелердің желі ішінде орналасқан өте маңызды және құпия компьютерлерге қол жетімділігін шектеуге тырысамыз.

DMZ үшін жалпы қол жетімділік ережелері сыртқы пайдаланушыларға демилитаризацияланған аймақтағы жүйелерде орналасқан тиісті қызметтерге қол жеткізуге мүмкіндік береді. DMZ жүйелері ішкі желілік жүйелерге қол жеткізуге қатаң шектеулер қояды. Мүмкіндігінше Ішкі жүйе мен DMZ арасындағы байланыс Ішкі жүйемен басталуы керек. Ішкі жүйелер саясатқа сәйкес DMZ-ге немесе Интернетке қол жеткізе алады, бірақ сыртқы пайдаланушыларға ішкі жүйелерге кіруге тыйым салынады.

2-суретте DMZ-де ұсынылатын қызметтер көрсетілген. Ішкі және сыртқы пошта серверлері бар екенін ескеріңіз. Сыртқы пошта сервері кіріс поштаны қабылдау және шығыс поштаны жіберу үшін қолданылады. Жаңа поштаны сыртқы пошта сервері қабылдайды және ішкі пошта серверіне жіберіледі. Ішкі пошта сервері Шығыс поштаны сыртқы серверге жібереді. Мінсіз жағдайда, бұл әрекеттердің барлығын ішкі пошта сервері сыртқы пошта серверінен пошта сұрай отырып орындайды.



2-сурет. DMZ және ішкі желі арасындағы жүйелер топологиясы

Кейбір брандмауэрлер пошта серверлерінің функцияларын орындай алады. Пошта сервері бар брандмауэрді пайдаланған кезде, соңғысы сыртқы пошта сервері ретінде жұмыс істейді. Бұл жағдайда сыртқы пошта сервері артық болады және оны жоюға болады.

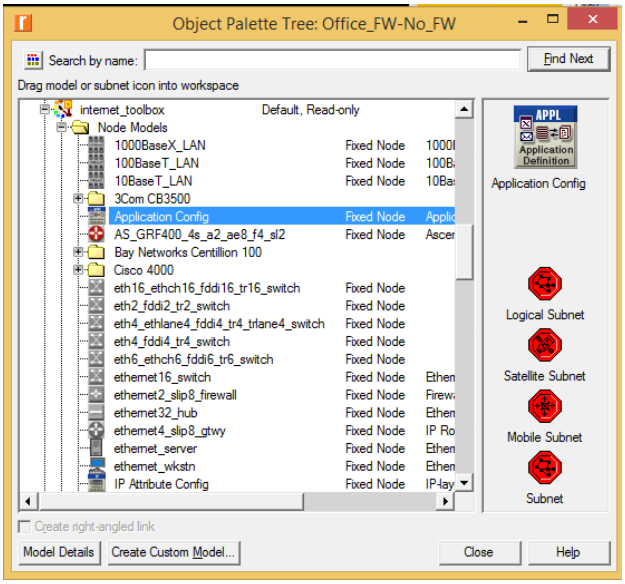
Жалпыға қол жетімді веб-серверлер қарусыздандырылған аймақта орналасқан. 2-суретте DMZ-де қосымшалар сервері көрсетілген. Көптеген веб-сайттар пайдаланушы енгізген деректер негізінде жұмыс істейтін белсенді мазмұнды қамтамасыз етеді. Пайдаланушы енгізген деректер өңделеді және қажетті ақпарат дерекқордан алынады. Деректер базасында маңызды ақпарат бар және оны қарусыздандырылған аймақта орналастыруға болмайды. Веб-Сервердің өзі дерекқор серверімен кері байланыс жасай алады, бірақ веб-сервер сыртқы ортадан қол жетімді және осылайша толық сенімге ие емес. Бұл жағдайда үшінші жүйені дерекқорға тікелей қосылатын қосымшаны орналастыру үшін пайдалану ұсынылады. Веб-сервер пайдаланушы енгізген деректерді алады және оны өңдеуге арналған бағдарлама серверіне ұсынады. Бағдарлама сервері дерекқордан қажетті ақпаратты сұрайды және оны пайдаланушыға жеткізу үшін веб-серверге ұсынады.

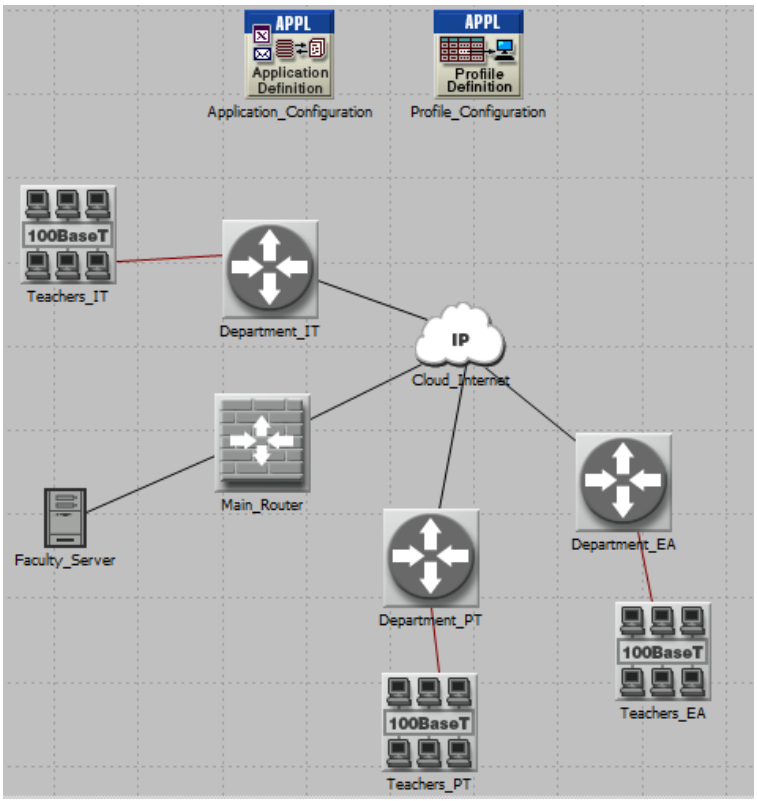
Бұл процесс күрделі болып көрінуі мүмкін, бірақ мұндай архитектура дерекқор серверін қорғауды қамтамасыз етеді және веб-Сервердің есептеу жүктемесін азайтады, өйткені веб-Сервердің сұраныстарды орындаудың қажеті жоқ.

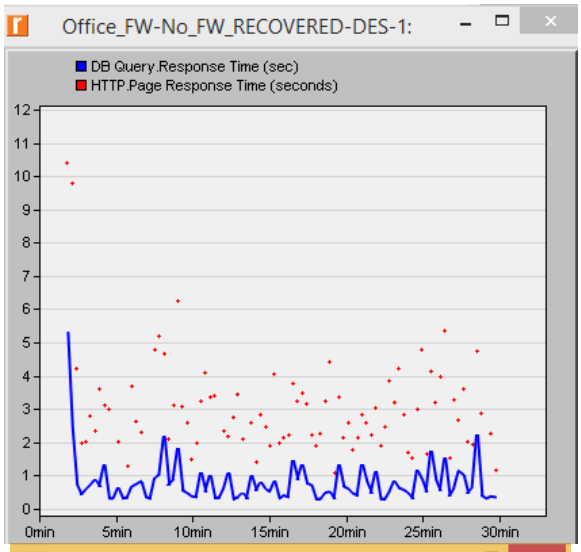
Дерекқор серверінде ұйым үшін өте маңызды ақпарат болуы мүмкін болғандықтан, оны басқа брандмауэрмен қорғаған жөн. Бұл жағдайда брандмауэр құпия дерекқорды ішкі желіден бөледі және осылайша оған қол жеткізуді одан әрі шектейді.

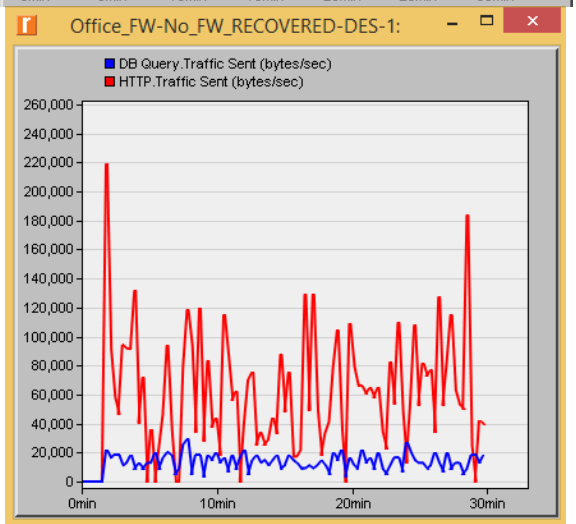
Сыртқы ортадан қол жетімді барлық жүйелер демилитаризацияланған аймаққа орналастырылуы керек. Сондай-ақ, егер жүйе интерактивті сессия арқылы қол жетімді болса (мысалы, *telnet* немесе *SSH*), пайдаланушылар DMZ-де орналасқан басқа жүйелерге қарсы шабуыл жасай алады. Мұндай жүйелер үшін DMZ-дегі басқа жүйелерді қорғау үшін екінші демилитаризацияланған аймақты құру орынды болуы мүмкін.

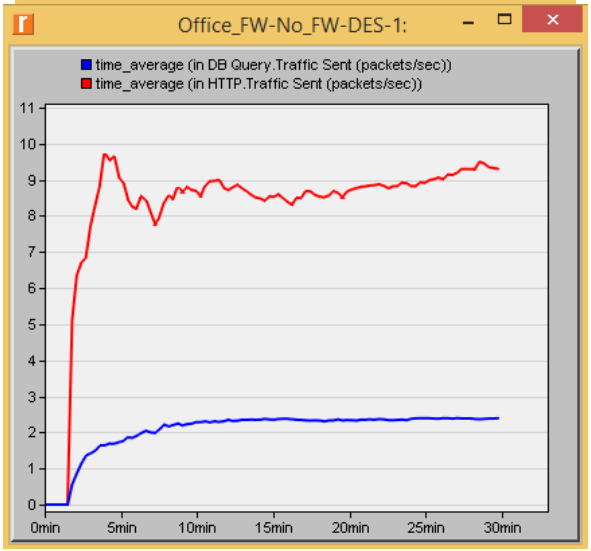
Мысал ретінде Riverbed Modeler Academic Edition эмуляторларында құрылған желі мысалын қарастырайық:


Object Palette Tree: Office_FW-No_FW
Search by name:
Find Next
Drag model or subnet icon into workspace
internet_toolbox
Default, Read-only
Node Models
1000BaseX_LAN
100BaseT_LAN
10BaseT_LAN
3Com CB3500
Application Config
AS_GRF400_4s_a2_ae8_f4_sl2
Bay Networks Centillion 100
Cisco 4000
eth16_ethch16_fddi16_tr16_switch
eth2_fddi2_tr2_switch
eth4_ethlane4_fddi4_tr4_trlane4_switch
eth4_fddi4_tr4_switch
eth6_ethch6_fddi6_tr6_switch
ethernet16_switch
ethernet2_slip8_firewall
ethernet32_hub
ethernet4_slip8_gtwy
ethernet_server
ethernet_wkstn
IP Attribute Config
Fixed Node
APPL
Application Definition
Application Config
Logical Subnet
Satellite Subnet
Mobile Subnet
Subnet
Create right-angled link
Model Details
Create Custom Model...
Close
Help


APPL
Application Definition
Application_Configuration
APPL
Profile Definition
Profile_Configuration
100BaseT
Teachers_IT
Department_IT
IP
Cloud_Internet
Main_Router
Faculty_Server
Department_PT
Department_EA
100BaseT
Teachers_EA
100BaseT
Teachers_PT


Office_FW-No_FW_RECOVERED-DES-1:
DB Query.Response Time (sec)
HTTP.Page Response Time (seconds)
12
11
10
9
8
7
6
5
4
3
2
1
0
0min
5min
10min
15min
20min
25min
30min


Office_FW-No_FW_RECOVERED-DES-1:
DB Query.Traffic Sent (bytes/sec)
HTTP.Traffic Sent (bytes/sec)
260,000
240,000
220,000
200,000
180,000
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
0min
10min
20min
30min


Office_FW-No_FW-DES-1:
time_average (in DB Query.Traffic Sent (packets/sec))
time_average (in HTTP.Traffic Sent (packets/sec))
11
10
9
8
7
6
5
4
3
2
1
0
0min
5min
10min
15min
20min
25min
30min