Осма глава
ЕКРАНИРАЩИ РУТЕРИ И ЗАЩИТНИ СТЕНИ

8.1 ВЪВЕДЕНИЕ

Защитните стени и екраниращите рутери са средства за ограничаване на трафика между две мрежи или към и от даден хост.

Целта на ограничаването е недопускането на определен трафик да бъде предаден от дадено мрежово устройство или да бъде получен от него. Ограничаването на трафика се извършва чрез предварително зададени дефиниции (rules). Правилата за ограничаване се прилагат върху пакетите, принадлежащи на съответния източник на трафик. Всяко правило определя дали пакетът може да постъпи или напусне съответната крайна система[1].

За описването на действието на защитните рутери и защитните стени е необходимо да се въведат някои основни понятия и обяснения[2].

8.2 ПОНЯТИЯ

Хост (Host) – Компютър, обменящ данни с други компютри (крайни системи) посредством комуникационна мрежа.

Гейтуей (Gateways) – Крайна система, функционираща над мрежовото ниво, съгласно OSI модела. Функцията й е да предава пакети между две мрежи.

Вътрешна мрежа - Сбор от всички комуникационни мрежи и хостове, обслужващи дейността на дадена организация или институция. В тази мрежа се намират всички ресурси и данни, които имат нужда от защита.

Външна мрежа. По принцип – всички останали мрежи и компютри, които не принадлежат на вътрешната мрежа.

Демилитаризирана зона (Demilitarized Zone, DMZ) – Мрежа, съдържаща публично достъпни компютри, на които са стартирани различни сървъри. Тя е добавена (вградена) между защитената вътрешна мрежа и външната мрежа с цел да осигури допълнителен слой в защитата. Тя е *изолирана* от вътрешната мрежа. Препоръчително е изолирането на тази зона и от външната мрежа. Другото й име е **гранична мрежа (Perimeter Network).**

Бастион (Bastion) Крайна система (хост), на която работят публично достъпни услуги[3] (сървъри). Бастионите се разполагат в демилитаризираната зона (граничната мрежа).

Филтриране (сканиране) на пакети (Packet Filtering) Действието, което дадено мрежово устройство предприема за да пропусне или спре трафик от и/или към дадена мрежа. Филтрирането е свързано с изпълнение на правила, които определят дали да се пропускат или блокират пакети, постъпващи или излизащи от мрежата. За да се осъществи пакетно филтриране, се съставя набор

---

[1] Хост или мрежово устройство.

[2] Материалът в тази глава е разработен на основа на материали [35,50] и авторите ги препоръчват на желаещите да вникнат задълбочено в проблема.

[3] Такава услуга е например електронна поща, или html достъп.

от правила, описващи какви типове пакети са допустими и какви да се блокират. Процесът на филтриране се извършва чрез прочитане (сканиране) на съдържанието на заглавната част на пакетите за съответните протоколи. Филтрирането на пакети може да се осъществи в маршрутизатор (router), мост (bridge) или отделен хост.

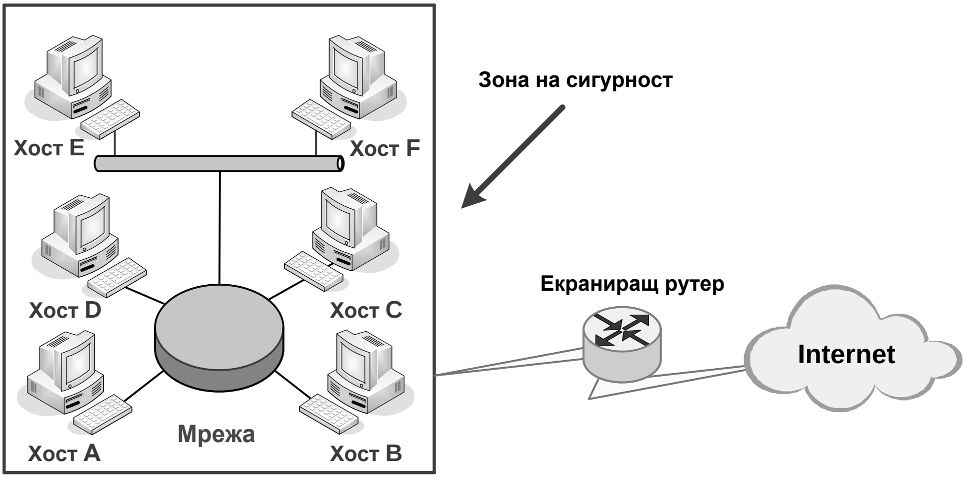
8.3 ЕКРАНИРАЩИ (ЗАЩИТНИ) РУТЕРИ

Екраниращият рутер сканира и анализира стойността на полетата от заглавните части на пакетите. Анализирането на данните представлява процес на:

- определяне на стойността на битовете в дадено поле на заглавната част на пакета (header);
- интерпретирането й в зависимост от спецификацията на конкретния протокол;
- сравнението на тази стойност с предварително дефинираните правила за нея;
- предприемане на съответното действие по допускане или унищожаване на пакета с данни.

Начинът за използване на екраниращ рутер е даден на Фиг. 8.1. Рутерът е използван за да отдели мрежата от Интернет. При това разделяне се дефинират две зони:

- зона на риск;
- зона на сигурност, доверена зона.

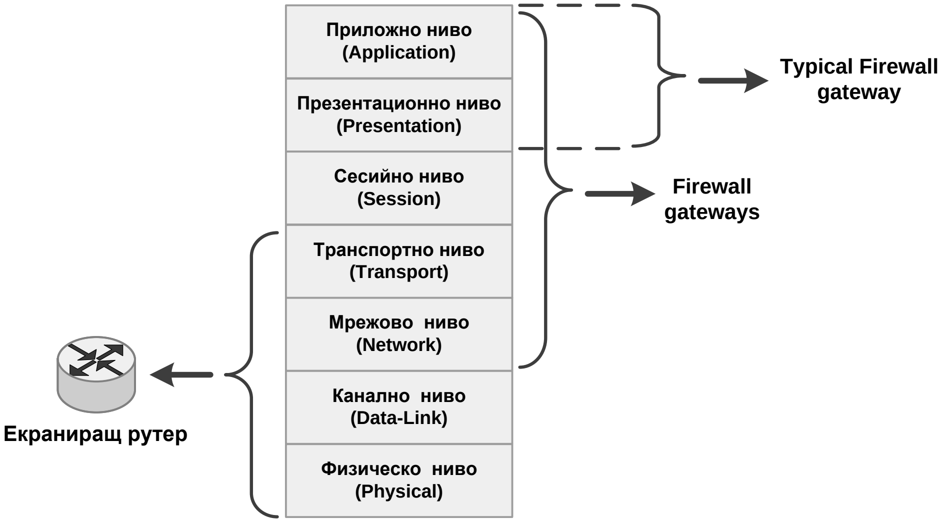


Фиг.8.1.Зона на сигурност.

Зоната на сигурност [35] включва хостове A,B,C,D,E,F. Зоната на риск включва в себе си хостовете, намиращи се извън нея. В случая това са компютри в Интернет. Рутерът се инсталира извън зоната на сигурност. В зоната на сигурност може да се намират една или повече компютърни мрежи.

Мрежа, която се намира в зоната на сигурност, се нарича „**вътрешна (защитена, сигурна) мрежа**”. Останалите мрежи се обединяват в термина „**външна мрежа**”. Разделянето на вътрешната от външната мрежа **не означава**, че вътрешната е окончателно и напълно защитена. Атаки в зоната на сигурност са напълно възможни и не могат да се изолират чрез защитния рутер, ако източника на интрузия е член на вътрешната мрежа.

Екраниращият рутер защитава вътрешната мрежа посредством **филтриране на пакети.** Филтрирането на пакетите се извършва преди постъпването им в защитената мрежа. Директното преминаване на пакетите между вътрешната и външната мрежа е **забранено**. Ако това стане, политиката за сигурност се счита за компрометирана. Думата „екраниращ рутер” показва нивото от OSI модела, на което се реализира защитата. Нивото, на което работи екраниращия рутер, е показано на Фиг.8.2 [35].



Фиг.8.2. Разположение на защитните средства съгласно OSI модела

Екраниращите рутери филтрират пакетите основно на *мрежово и транспортно* ниво, докато защитните стени[4] функционират аналогично на гейтуей (gateways). Съществуват варианти на екраниращите рутери, които могат да извършват филтрация на канален и физически слой. От своя страна съвременните защитни стени се произвеждат с възможности за филтриране на всички седем нива на OSI модела, поради което границата между тях и защитните рутери се размива.

Посредством анализа на пакети, наложен върху сегментите в транспортния слой, мрежовите рутери могат да определят и възможността за съществуване на услугите (използващи този слой) в дадена крайна система. В

---

[4] Подробно описание на защитните стени и екраниращите рутери е дадено в [35].

транспортното ниво (TCP, UDP) сканирането на пакетите е свързано с определяне на портовете, на които се търсят съответните услуги (Service Access Point). Транспортното ниво е отговорно за създаване на логическите (виртуални) канали.

Сканирането на заглавните части на протоколите от транспортния слой - в случая TCP, е концентрирано върху следните полета:

- порт на подателя на пакета;
- порт на получателя на пакета;
- флагове за установяване на сесия.

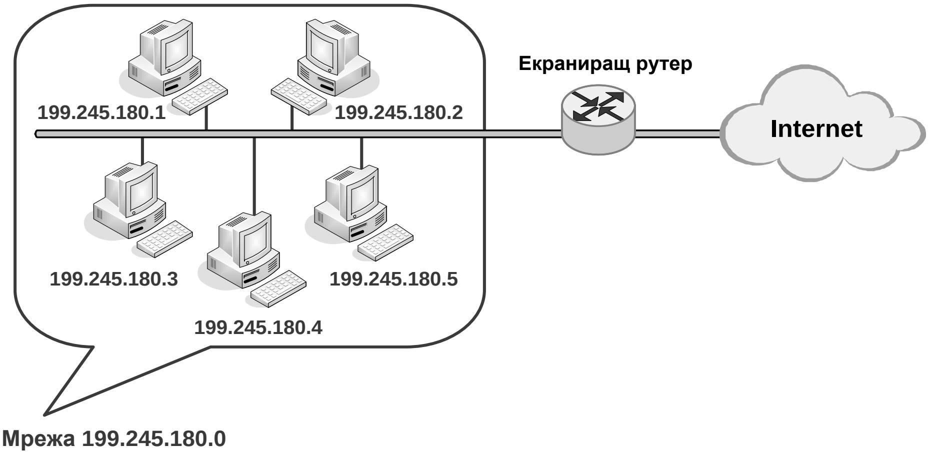
Правилата за филтриране на пакети са отражение на политиката за сигурност, която се възприема от съответната организация. Дефинирането на правила за филтриране може да се реализира на следните стъпки:

1. За всеки порт на защитният рутер се дефинират правила за пакетна филтрация.
2. При пристигане на пакет на порта се прави сравнение на хедърите на протоколите на пристигналия пакет с дефинираните правила за филтрация.
3. Всяко правило се прилага по предварително определен ред.
4. Ако пакета отговаря на правило за пропускане – той се пропуска в зоната на сигурност.
5. Ако пакета отговаря на правило за отхвърляне – той се отхвърля и не влиза в зоната на сигурност.

В процеса на дефиниране на правила е задължително да се спазва следния принцип при определянето на критериите за отхвърляне на пакет:

ВСИЧКО, КОЕТО НЕ Е СПЕЦИАЛНО РАЗРЕШЕНО, СЕ СЧИТА ЗА ЗАБРАНЕНО.

8.4 ПРОЕКТИРАНЕ НА ПРАВИЛА ЗА ФИЛТРИРАНЕ НА ПАКЕТИ



Фиг 8.3. Мрежа, защитена с екраниращ рутер.

Дадена е мрежа с конфигурация показана на Фиг. 8.3. В тази мрежа има необходимост да се използват услуги от тип електронна поща. Съществува хост с име BADBOY (в зоната на риск, Internet), по отношение на който дефинираме рестриктивна политика на сигурност. Рестрикциите се изразяват в забрана за получаване на пакети от него в зоната на сигурност (мрежа 199.245.180.0). Необходимо е също така, хостовете от мрежата да имат възможност за връзка до WWW-сървър.

Правилата за филтриране се описват в таблица 8.1[35].:

Таблица 8.1

Номер на правило	**Действие**	**Хост на вътрешна мрежа**	**Порт на хоста**	**Външен хост**	**Порт на хоста**	**Посока**	**Описание**
1	Стоп	*	*	BADBOY	*	*	Блокиране на трафика от BADBOY
2	Премини	WWW-GW	80	*	*	*	Разрешаване на достъпа до WWW гейтуея
3	Премини	*	*	*	25	*	Разрешаване на излизащия трафик към отдалечения пощенски сървър

Записите в таблицата имат следния смисъл:

Правило 1 притежава описан един хост в полето „Външен хост”. За него действието на екраниращия рутер е „Стоп” по отношение на всеки негов порт. Следователно правилото има следния смисъл: *Блокирай създаването на сесии от хост BADBOY към всяка машина (*) и всеки негов порт (*), принадлежащ на вътрешната мрежа и в двете посоки..*

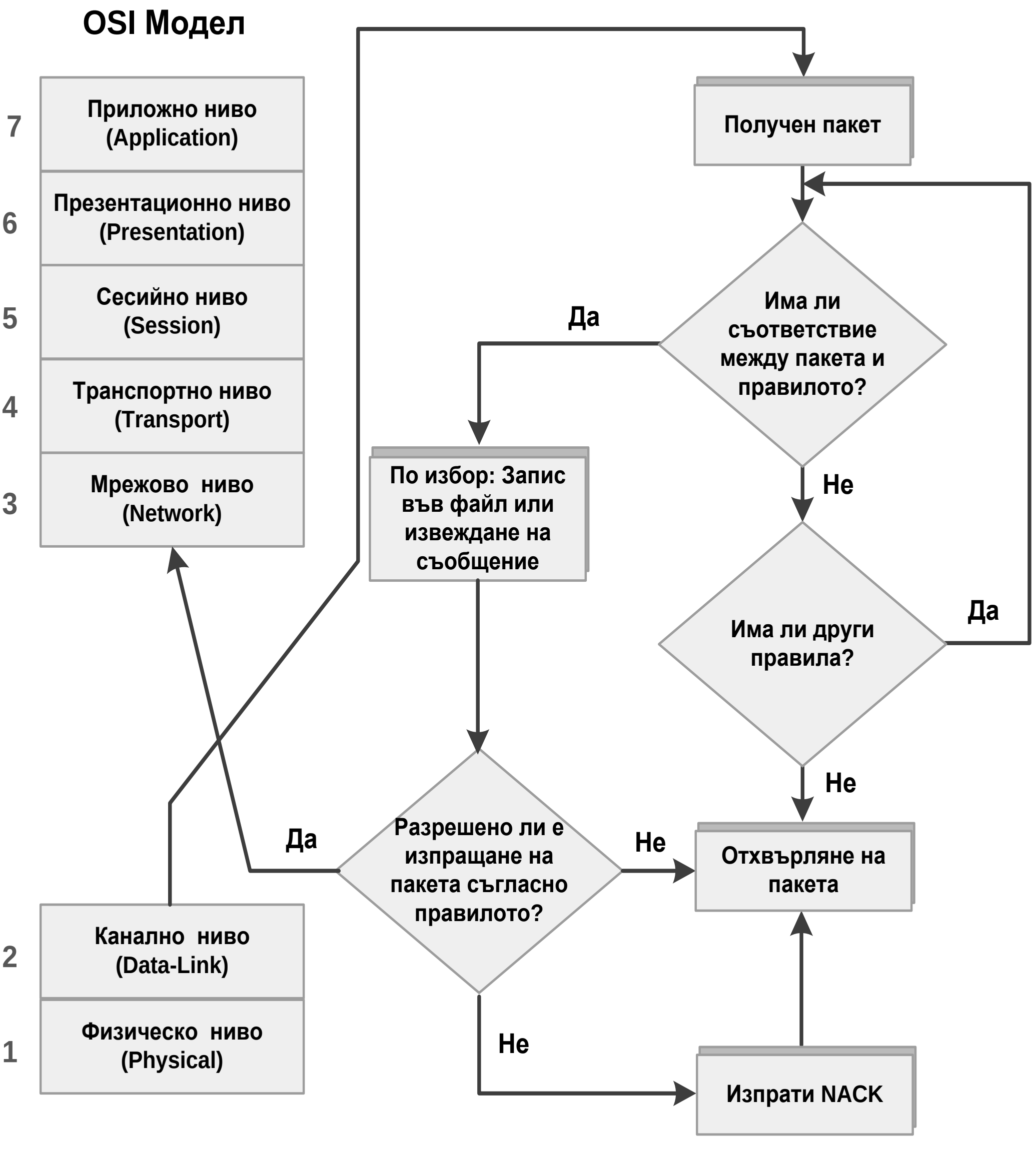
Правило 2 е разрешаващо, понеже в полето „Действие” е записана операция за пропускане на трафик. Тази операция е дефинирана за всеки хост и порт. Правилото има следния смисъл: *Пропусни всеки пакет, изпратен от произволен порт (*) на произволен хост (*) към гейтуея за WWW услуги (WWW-GW), в двете посоки.*

Правило 3 дава разрешение на всеки хост, член на зоната на сигурност, да изпраща пакети до порта за електронна поща.

Филтрирането на всеки пакет се извършва в момента на постъпването му на конкретен порт на екраниращия рутер. Филтрирането се извършва по следния алгоритъм[35], представен на фиг. 8.4. Входящият пакет се получава от каналния слой[5] и се подлага на анализ за съответствие с дефинираните правила.

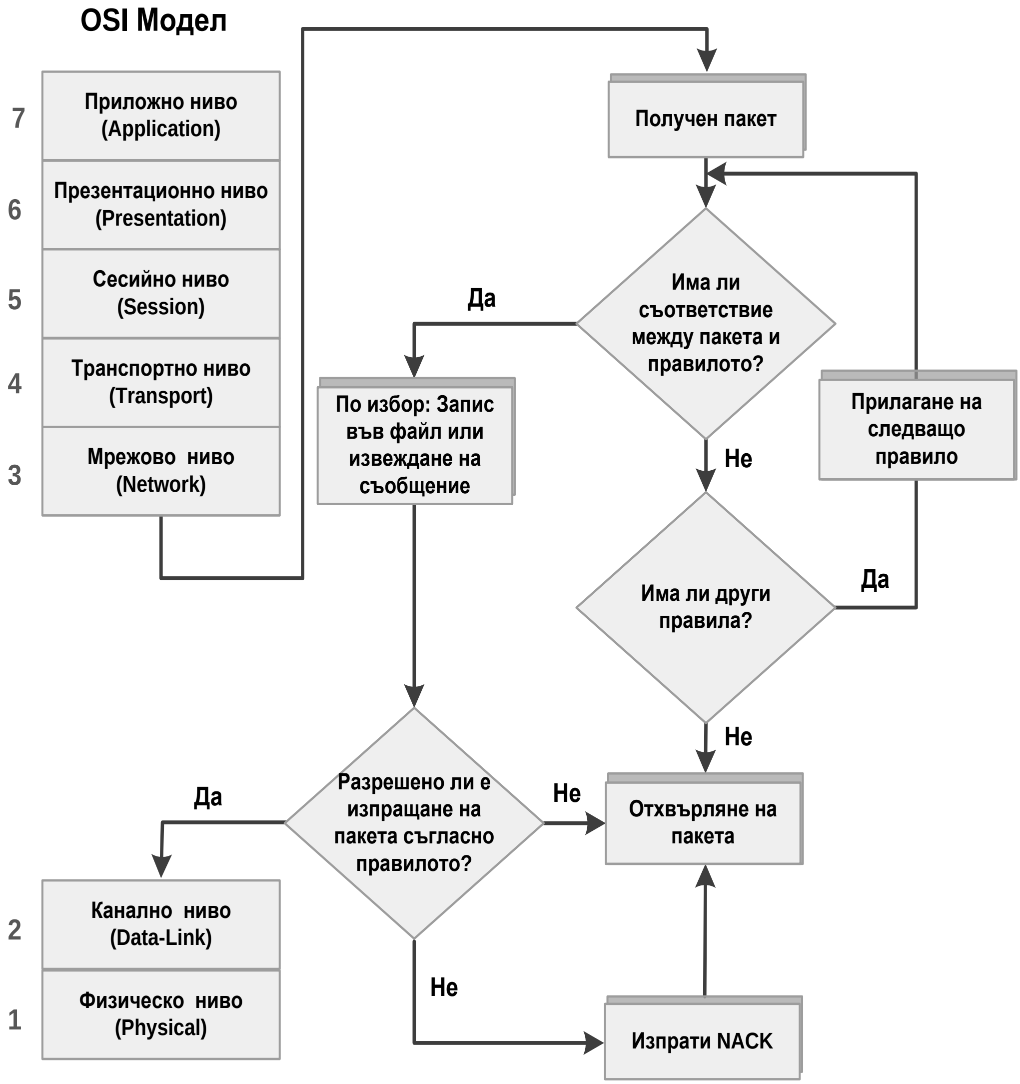
---

[5] Ethernet картата.



Фиг. 8.4. Филтриране на входящи пакети

При филтриране на изходящият трафик, показан на Фиг. 8.5. анализът на пакета се извършва преди изпращането му в каналния слой.

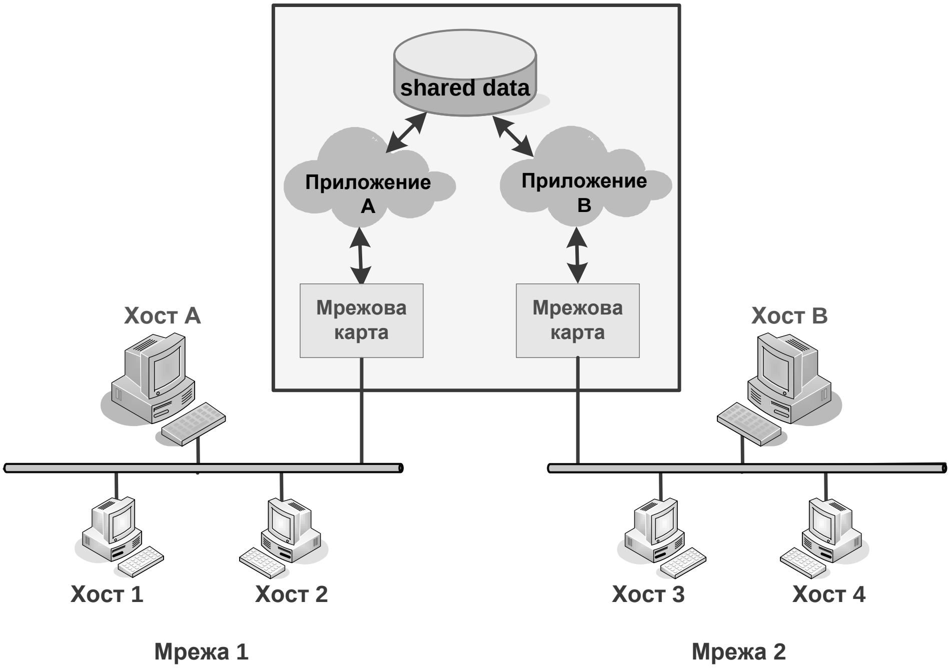


Фиг. 8.5. Филтриране на изходящи пакети.

Изпращането на NACK се извършва от защитната стена. NACK се изпраща до комуникационният стек на хоста, изпратил този пакет. При получаването му стекът трябва да изработи съобщение, с което да уведоми ползващата го програма за възникналия проблем.

8.5 АРХИТЕКТУРИ НА ЗАЩИТНИ СТЕНИ

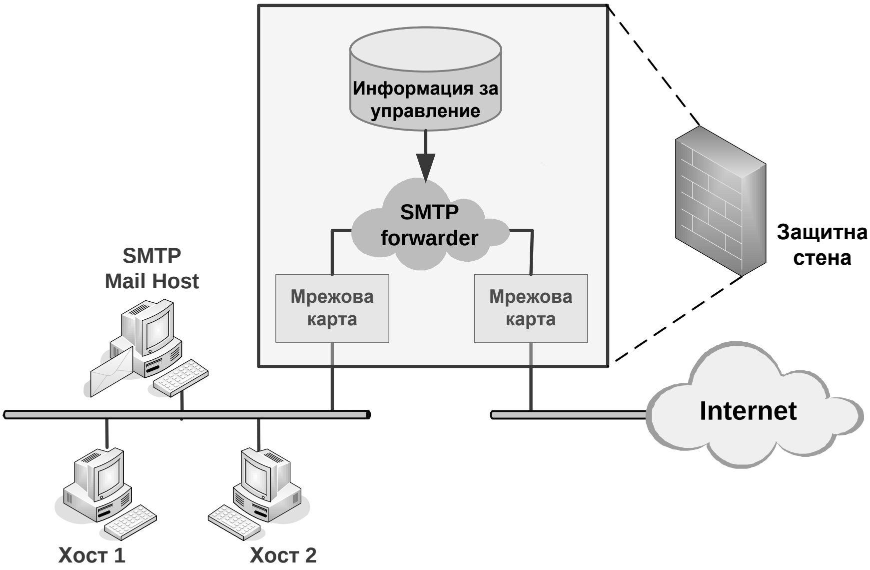
8.5.1. Dual-homed host (DHH)



Фиг 8.6. Хост с две мрежови карти.

Dual-homed host е хост с два мрежови интерфейса (две мрежови карти – фиг. 8.6). Между двете карти трафикът на пакети може да е забранен или разрешен. Ако е забранен, остава единствения вариант за обмен на данни, посредством програми (процеси), стартирани от операционната система на общата точка за връзка. В случая това е DHH. В този хост данните могат да се обменят единствено в апликационния слой.

Ако в DHH са конфигурирани услуги от типа на електронна поща и WWW сървър, то за да се осигури работата им едновременно в зоната на риск и зоната на сигурност, е необходимо тези услуги да заобикалят правилта на защитната стена. От тази гледна точка, може да се очаква, че ще се налага част от потребителите да достъпват директно хоста със защитната стена. Процесът на директно достъпване предполага възможност за директно предаване на трафик между вътрешната и външната мрежа. Това тяхно действие може да доведе до сериозно компрометиране на дейността на стената по отношение на филтриране на останалия трафик. Затова е необходимо конфгурирането на всички услуги, управляващи трафика в DHH хоста, да е подчинено на правилата на стената. За целта се прилага вариант за филтриране на трафика представен на Фиг. 8.7.



Фиг 8.7. Разполагане на защитна стена върху два интерфейса

DHH приема пакетите от мрежовия интерфейс, свързан към Internet, прилага върху тях правилата за филтриране и ги изпраща към програмата, отговаряща за препредаване на електронната поща (SMTP forwarder) към вътрешната мрежа.

Недостатък, по отношение на мрежова функционалност, на DHH е липсата на маршрутизиращи (рутиращи) функции, поради което единствения път между два мрежови сегмента е посредством функциите на приложния слой (Application Layer). Липсата на рутиращи функции е наложена от политиката за сигурност и е задължителна. При инсталиране на DHH е **задължително да се изключи рутиращата функция** в конкретната операционна система.

Най-голямата заплаха за компрометиране на политиката на сигурност на DHH е възможността за директен достъп (direct login access) на интрудера до хоста. Такава възможност съществува при наличие на допълнителна (прокси[6]) услуга (application proxy) в DHH. За да не се допуска възможност за реализиране на тази заплаха е задължително достъпът до DHH да се извършва или през локална конзола, или криптиран отдалечен достъп (secure remote access).

Последиците от успешна интрузия срещу DHH е отварянето на вътрешната мрежа по отношение на входящия и изходящия трафик. Вътрешната мрежа остава незащитена и се създава заплаха за вероятна интрузия срещу данните и ресурсите, намиращи се на хостовете в нея.

За да се минимизира вероятността за успешна интрузия, е необходимо да се премахнат от DHH всички ресурси, който могат да бъдат използвани за тази цел. Такива са:

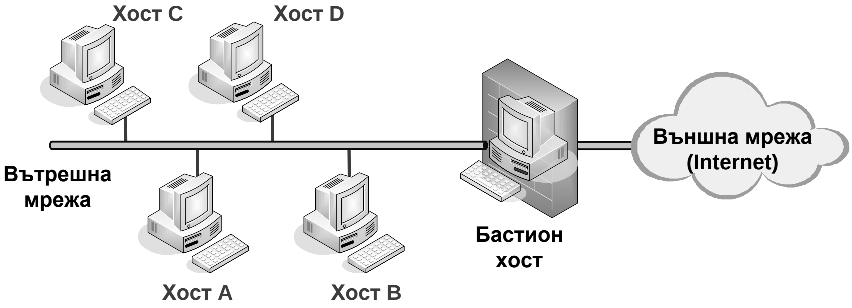
---

[6] Прокси услугата е обяснена на фиг. 8.17.

- компилатори и линкери;
- програми, служещи за промяна на нивото на сигурност;
- мрежови услуги, които няма да се ползват или противоречат на политиката за сигурност (например ftp услуга);
- стартови системни скриптове, който активират ненужни услуги.

8.5.2. Bastion host

Бастион-хостът е защитен хост, критичен по отношение на мрежовата сигурност. Бастион-хостът е компютър, управляващ входящия и изходящия трафик в дадена мрежа с възможности за филтрация на всички нива от OSI модела. Реализирането на бастион хост е показано на Фиг. 8.8.



Фиг. 8.8 Разполагане на бастион хост.

За означаване на бастион хостовете е въведена следната нотация [35]:

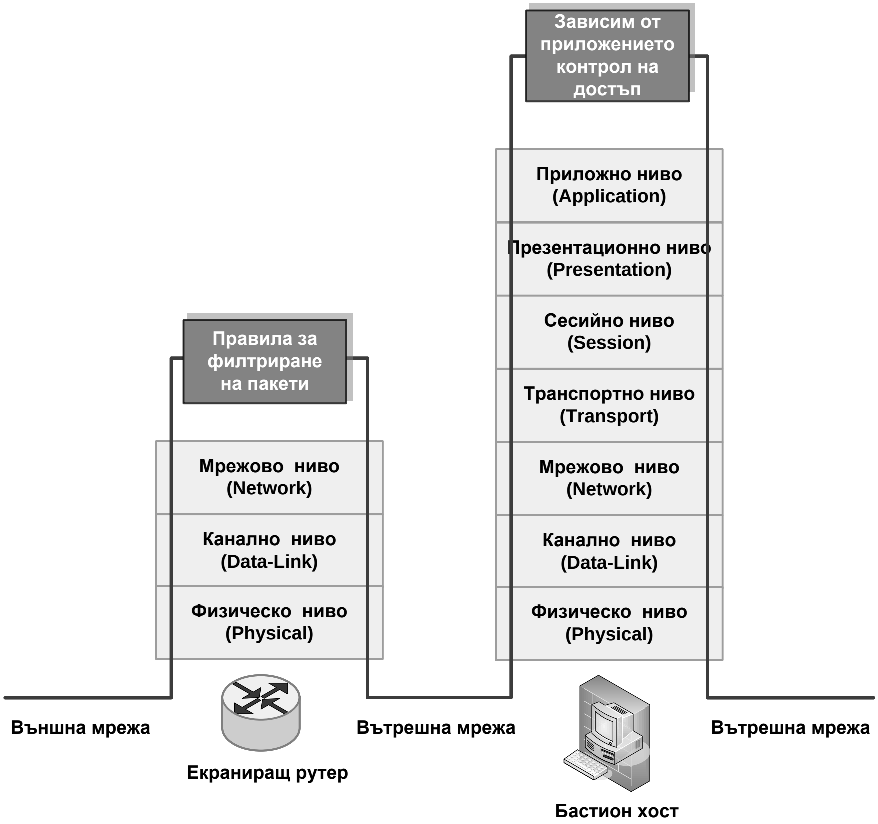
Символ	Описание
S	Екраниращ рутер
R	Обикновен рутер
F1	Защитна стена с един мрежов интерфейс
F2	Защитна стена с два мрежови интерфейса
B1	Бастион хост с един мрежов интерфейс
B2	Бастион хост с два мрежови интерфейса

8.5.3. SCREENED HOST GATEWAY

Бастион-хостът е първа линия на защита между зоната на риска и доверената зона. Като възможен вариант за изтегляне на бастион-хоста на втора линия и предварителната му защита от атаки, е вариант за реализация, показан на Фиг. 8.9.

Фиг. 8.9. Схема на защита чрез бастион хост и екраниращ рутер.

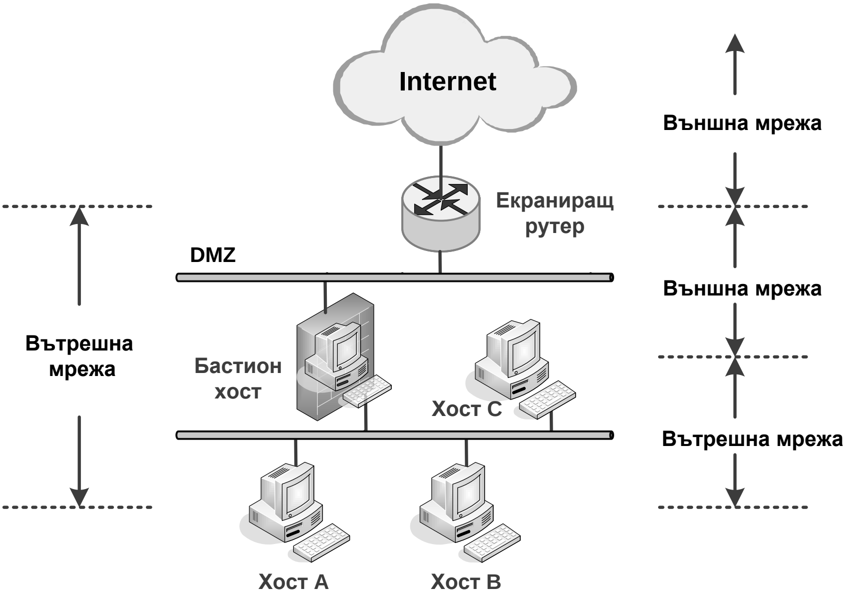
В случая екраниращия рутер е конфигуриран така, че да изпраща целия трафик след филтрация в бастион хоста. В бастион-хоста трафикът минава на втора филтрация, която обхваща вече и програмите, работещи с приложния слой (Application Layer). Тази схема е по-добра от първата. При евентуален пробив в защитния рутер, интрудерът попада на бастион-хоста. Идеологията на двукратното филтриране на трафика е представено на фиг.8.10



Фиг. 8.11 Разполагане на защитни средства от гледна точка на OSI модела

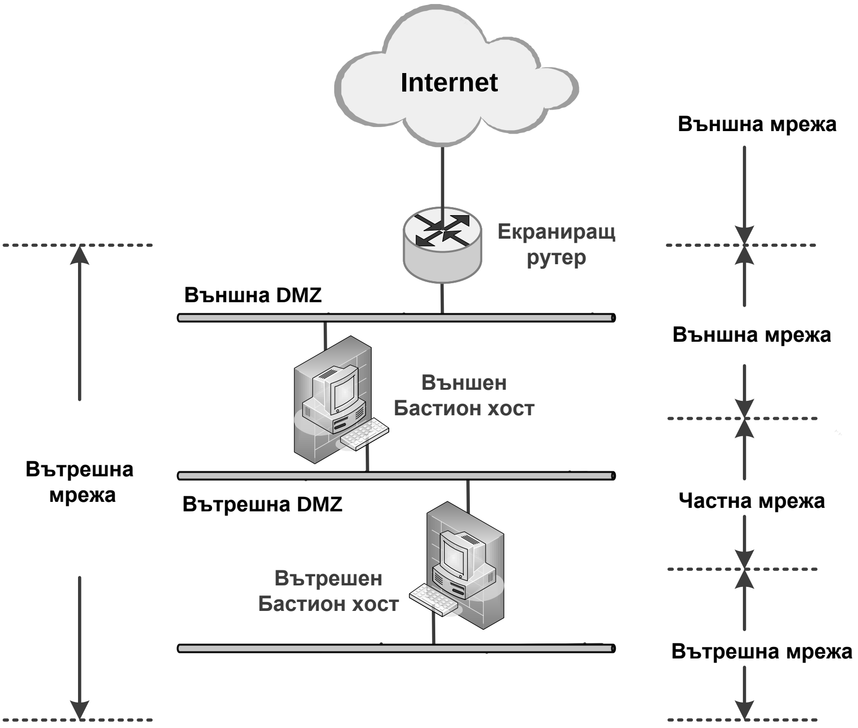
Целият входящ трафик от външната мрежа се насочва към един порт на екраниращия рутер. След като премине през филтрация, изходящия трафик се насочва само към един порт на бастион хоста, където минава на втора филтрация. Тя включва в себе си филтриране на приложно ниво за определяне на правата за достъп до вътрешната мрежа на трафика, постъпващ от външната мрежа. Трафикът, генериран от вътрешната към външната мрежа (outgoing traffic), може да се пренасочи директно към екраниращия рутер. В този аспект на дейността си, бастион-хостът изпълнява функции на гейтуей. Затова тази схема на защита се нарича **screened host gateway**.

На Фиг.8.12 е показана конфигурация на бастион-хост и екраниращ рутер, ползващи по два мрежови интерфейса (мрежови карти). Едната мрежова карта на екраниращия рутер приема постъпващия трафик от външната мрежа и го пренасочва след филтрация към втората си мрежова карта, свързана с демилитаризираната зона. Рутиращата таблица на екраниращия рутер е конфигурирана така, че втората интерфейсна карта да изпраща трафика, постъпващ към нея единствено към първата мрежова карта (интерфейс) на бастион-хоста. Така се гарантира постъпването на трафика в Dual-homed host -та да става единствено към определен хост и на предварително определен порт в него. След филтриране, бастион-хостът препредава трафика към вътрешната мрежа, посредством втория си мрежов интерфейс. Тази схема може да се отбележи с нотация S-B2 [35].



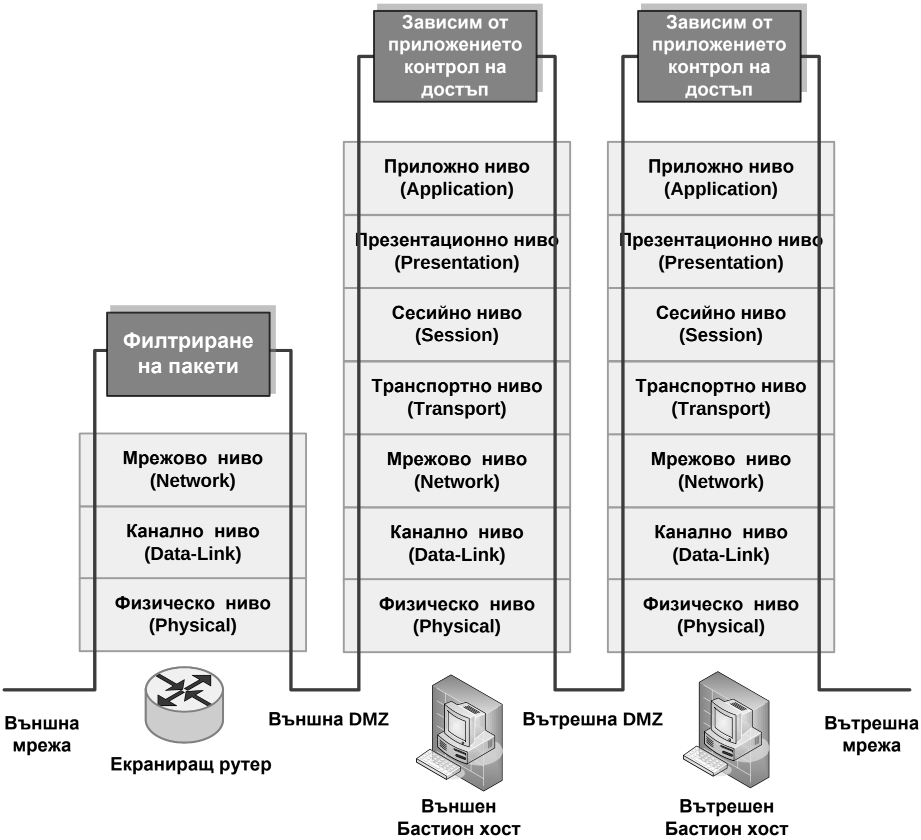
Фиг. 8.12 Сегментиране на вътрешна мрежи.

Един от основните проблеми на защитата е намаляването на вероятността за заплаха и/или атака от вътрешната мрежа, целяща компрометиране на сигурността на бастион-хоста или екраниращия рутер. При провеждане на успешна атака интрудерът ще осигури безпрепятствен достъп в двете посоки на трафика от външната мрежа и така ще си осигури ресурс за провеждане на втора атака, насочена към хостовете във вътрешната мрежа. За да се предотврати тази заплаха, е необходимо да се филтрира не само входящия от външната мрежа трафик, но и изходящия от вътрешната мрежа трафик. За целта бастион-хоста се разделя от вътрешната мрежа посредством организиране на междинна мрежа. Нотацията за записване на тази конфигурация е S-B2-B2 [35]. Схемата за реализация на това решение е представена на фиг. 8.13.



Фиг. 8.13. Създаване на вътрешна мрежа в демилитализирана зона.

Входящият трафик от външната мрежа постъпва в екраниращия рутер, през мрежовия му интерфейс, свързан към външната мрежа. Трафикът се филтрира и се изпраща през втория интерфейс към първата мрежова карта на външния бастион-хост. Там се прилага филтриране, обхващащо всички нива на OSI модела. Изчистения трафик се изпраща към интерфейса на вътрешния Бастион-хост, свързан към външната демилитаризирана зона. Той извършва второ филтриране на трафика и след това го изпраща през втория си интерфейс към вътрешната мрежа. В обратна посока – изходящ трафик от вътрешната към външната мрежа, трафикът постъпва първо във вътрешния бастион-хост и едва след филтрация се изпраща към външния бастион-хост. В процеса на филтрация се отстраняват всички възможни пакети в приложното ниво, представляващи заплаха за работата на външния бастион- хост. Схемата на филтриране от гледна точка на OSI модела е показана на Фиг. 8.14.



Фиг. 8.14. OSI модел на демилитализирана зона.

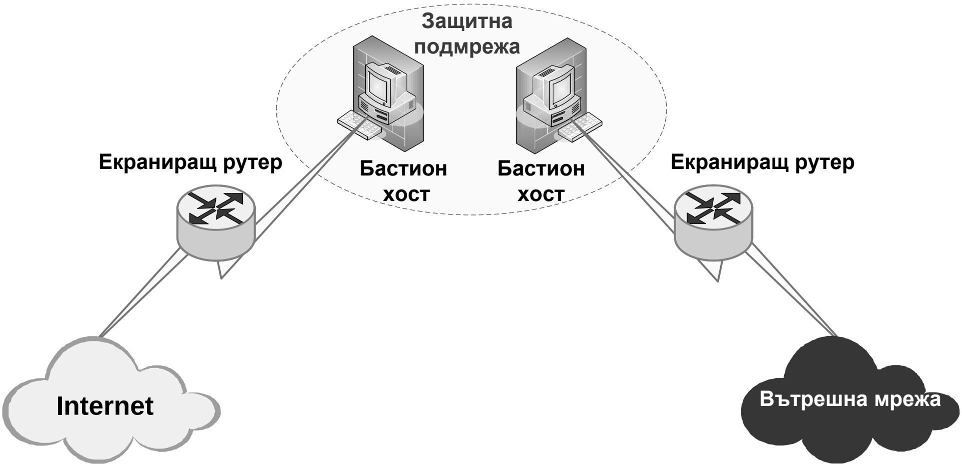
Увеличаването на степента на защита е свързано с изграждането на защитна подмрежа.

8.6 ЕКРАНИРАЩА ПОДМРЕЖА

Функцията на екраниращата подмрежа е да осигури цялостен изолиращ слой между зоната на риска и зоната на сигурност. Целта на тази мрежа е да не позволи директното предаване (forwarding) на трафик между двете зони. Входящият мрежов трафик постъпва в изолираната мрежа, там се филтрира и препредава от името на екраниращата подмрежа към вътрешната мрежа.

За да се реализира тази функционалност е необходимо разделянето на външната, екраниращата и вътрешната мрежа по начин представен на Фиг.8.15. Трафикът от външната мрежа постъпва на определени портове на екраниращия рутер, който го филтрира и изпраща към определен порт на бастион-хост в екраниращата подмрежа. Бастион-хостът филтрира трафика и може да го изпрати за допълнителен анализ в специализирани хостове, разположени в екраниращата подмрежа. След като трафика бъде филтриран, той се изпраща на бастион-хоста, свързващ екраниращата мрежа с вътрешната мрежа. От там трафикът постъпва в последната. Смисълът на тази защита е, че дори при успешна атака на първия бастион-хост, интрудерът попада в екраниращата мрежа. Там той трябва да преодолее защитата на специализираните хостове в нея, за да може да достигне до втория екраниращ рутер.

Ако успее да го преодолее, интрудерът има достъп до вътрешната мрежа. Ако правилно е проектирана и изпълнявана политиката на сигурност, вероятността за провеждането на такава успешна атака е много малка.



Фиг. 8.15.Реализиране на защитна подмрежа.

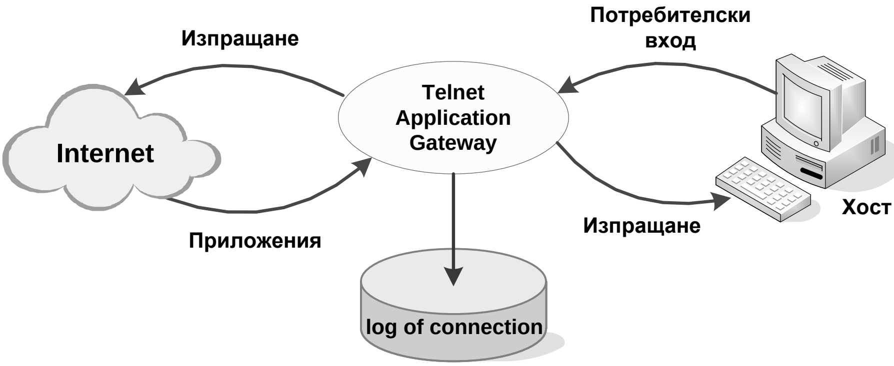
Едно от основните преимущества на използването на екраниращa подмрежа е пълното скриване на IP адресите на съответната вътрешна мрежа и избягването на възможността за директна атака, насочена към нея. В този случай адресът, с който официално се участва в интернет комуникациите (известни в Network Information Center), е IP адреса на първия бастион-хост, отнасящ се за интерфейса, който го свързва с Internet. В този случай бастион-хостът се ползва и като гейтуей на приложно ниво (Application Layer Gateway). Екраниращата мрежа и вътрешната мрежа могат да ползват локални IP адреси.

8.7 ЗАЩИТА НА АПЛИКАЦИОННО (ПРИЛОЖНО) НИВО (APPLICATION LEVEL GATEWAYS - ALG)

Програмите, осигуряващи защитата в седми слой на OSI модела, имат възможност за филтрация на трафика на приложно ниво. Те са програмирани така, че да могат да провеждат интелигентен (контекстно зависим) анализ на протоколите от приложния слой. Такъв пример е даден на Фиг. 8.16. Даден хост иска да ползва мрежова услуга „telnet”[7]. За целта се използва гейтуей за управление на тази услуга, като в процеса на управление се записват действията на потребителя на ниво команда.

---

[7] Отдалечен достъп в команден режим.



Фиг. 8.16. Защита на апликационно ниво.

Това е нов аспект по отношение на разглежданите до момента схеми за защита. Гейтуеят на приложно ниво има способност да филтрира, понеже има пълна информация за използвания протокол от 7 ниво на OSI модела. Той „разбира” подаваните от потребителските програми команди, понеже те използват разработени и известни API функции (интерфейси) за достъп до приложния слой.

Друг важен аспект по отношение на сигурността е възможността на програмите от тип Application Level Gateway да осигуряват контрол на достъпа до протоколите от приложния слой на потребителските приложения от операционната система. Те могат да забраняват или да разрешават на определени приложения ползването на комуникационния стек протоколи. На всяка програма (application), която иска да комуникира с протоколния стек, защитната стена присвоява идентификационен номер (ID). Стратегията на защитата се базира на дефиниране на правила за работа, свързани с този номер. Присвояването на номерата е случайно за всяка машина и трудно може да бъде определено при интрузия. За да се използва ALG защита, е необходимо софтуерът да се инсталира на всяка отделна машина и конкретния потребител да се автентифицира пред програмата и на базата на паролата да се активират правилата, определени за него. Друг вариант на употреба е възможността да се централизира защитата на една машина, която да изпълнява ролята на сървър, а на останалите да се сложи програма, която да работи като клиент на сървъра.

Защитни стени за персонални компютри могат да се осъществят по различни варианти. Стените се различават помежду си предимно по два основни параметъра:

- до какво ниво на OSI модела могат да разрешават филтриране;
- колко е гъвкава схемата за определяне на правила за работа на различните приложения и потребители.

Без да се претендира за пълна изчерпателност, тук е представен примерен алгоритъм за конфигуриране на защитна стена, която ще работи на персонален компютър.

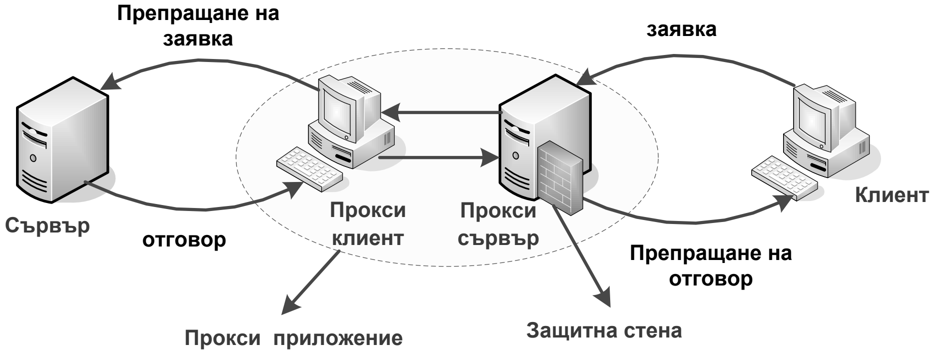
Вербален алгоритъм за построяване на филтриращо правило за приложно ниво:

1. Избор на име на правилото.
2. Определя се вида на правилото, дали да е разрешаващо или блокиращо.
3. Определя се за кои мрежови интерфейси (карти) се отнася.
4. Определя се трафика дали да се записва във файл или не.
5. Определя се множеството хостове за които се отнася правилото. Хостовете могат да се дефинират по IP адрес, MAC-адреси, маска на мрежата.
6. Определят се портове и протоколите от съответните комуникационни слоеве, за които се определя това правило.
7. За всеки порт и протокол се определят посоката на трафика, за което се прилага това правило.
8. Определя се периода от време, за който е валидно правилото.
9. Определя се за кои програмни продукти (applications) се прилагат тези правила.

При филтриране на приложно ниво може да се зададе конкретно правило за филтриране за всяка програма, която иска да ползва приложния слой. За целта ALG присвоява уникален код на програмата, ползваща приложния слой. Към този уникален код се присвоява филтриращото правило. При стартиране на програмата, ALG я идентифицира еднозначно и прилага за всички нейни пакети предварително дефинираните правила. По подразбиране ALG трябва да забранява достъп до приложния слой на всяка програма, която се опитва да изпраща пакети, ако за тази програма няма разрешаващо правило за исканите от нея операции. За да използва ALG, е необходимо потребителят да се автентифицира пред него. Това може да стане или чрез директно ползване на афтентификационна схема или чрез допълнителен специализиран клиент, който работи на потребителската машина и осъществява сигурна комуникация с хоста, на който работи Application Level Gateway.

Някои специфични програми изпълняват защитни функции като работят в режим на „прокси”. Прокси сървърите са специализирани приложения, стартирани на хост, изграждащ защитната стена (или DHH хост с интерфейси към вътрешната и външната мрежа, както и бастион-хост, достъпен, освен от Internet, и от вътрешни машини). Тези програми приемат потребителските заявки за комуникационни услуги (като FTP или Telnet) и, съобразявайки се с набор от правила, подчинен на политиката за сигурност, ги препращат или не на истинските сървъри или клиенти в мрежата.

Прокси сървърите работят в прозрачен режим по отношение на своите клиенти. Прозрачността е най-полезната черта на прокси сървърите. Чрез нея отдалечения сървър/хост, намиращ се във външната мрежа (зона на риска), получава всички заявки от прокси сървъра и ”вижда” само неговия адрес, но не и адресите на хостовете, генериращи заявките. Прокси услугите са ефективни, само ако се ползват съвместно с механизъм, ограничаващ директната комуникация между вътрешни и външни хостове. Дуал-хоум хостовете и системите за филтриране на пакети са два такива механизма. Ако вътрешните и външни хостове могат да комуникират директно, то те ще го правят, заобикаляйки прокси сървъра.



Фиг.8.17. Защитна стена изградена чрез прокси сървър.

Прокси услугата (Фиг. 8.17) изисква два компонента: прокси сървър и прокси клиент. Прокси клиентът е специална версия на нормална клиентска програма, проектирана да работи с прокси, наместо с истински сървър. Клиентската програма приема пакетите, пристигащи от сървърите, и след филтриране ги предава на прокси сървъра за изпращане във вътрешната мрежа. При получаване на заявка за изграждане на сесия от страна на вътрешната мрежа прокси сървърът изгражда тази сесия с желания адрес от външната мрежа като изпраща пакети от свое име. При успешно осъществяване на сесията прокси сървърът препраща получените пакети към хоста, поискал услугата. Преди да ги препрати той прилага върху тях филтриращите правила.

Важно е да се разбере, че прокси услугата сама по себе си е комуникационно софтуерно решение, а не архитектура на защитна стена, въпреки че изглежда такава поради ограниченията, които може да наложи на вътрешните потребители.

При разработване на прокси сървъри е необходимо да се проектира работата им така, че да функционират в режим „fail-safe”. Особеното на този режим е, че при неуспешно идентифициране на клиентските програми прокси сървърът не бива да компрометира защитните стени или екраниращите рутери.

Правилното решение при изграждане на защитна стена рядко е в самостоятелни схеми, ползващи един продукт. Използването на комбинация от различни технологии решава комплексно проблемите, свързани с изпълнението на политиката по сигурността. Някои протоколи като Telnet (Virtual Terminal Protocol) и SMTP (Simple Mail Transfer Protocol) се поддържат по-лесно с филтриране на пакети. Други, като FTP (File Transfer Protocol) и HTTP (Hyper Text Transfer Protocol), е по-добре да се оставят на прокси сървъра.

8.8 КАКВО НЕ МОЖЕ ДА ПРАВИ ЗАЩИТНАТА СТЕНА?

Защитните стени предлагат високо ниво на защита против опасностите в мрежата и крайните системи, но те не са цялостно решение. Определени заплахи са извън техния контрол. Срещу тях е необходимо да се предвиждат други решения.

Защитната стена не предпазва от атаки, насочени към изнасяне или унищожаване на информация, извършвани без ползване на мрежовите комуникационни ресурси.

Добре конфигурирани защитна стена, mail, web и ftp сървъри, силно се намалява вероятостта един пълноправен вътрешен потребител да изнесе поверителна информация по мрежов път. Но ако той да я копира на преносим носител и да я изнесе, защитната стена не може да го спре. Предотвратяване на вътрешните заплахи изискват вътрешни мерки за сигурност като хост защита, обучение на потребители, охрана от физически лица и др.

Защитната стена не може да предпази от връзки, които не минават през нея.

Защитната стена ефективно контролира трафика, минаващ през нея, но не може да направи нищо за този, който я заобикаля. Например, ако е разрешен dial-in достъп до системи, предлагащи Internet услуги, защитната стена не може да прихване тези пакети.

Решението на този проблем е в областта на обучението на персонала и правилното представяне на фирмената политика по отношение на сигурността.

Защитната стена не може да предпазва от неизвестни, нови заплахи.

Защитната стена се проектира, за да неутрализира известни интрузионни действия. Ако е добре конфигурирана, тя *би трябвало* да осигури защита и от абсолютно непознати заплахи. Например, ако по подразбиране се забрани целия Internet трафик, след което се разрешат само няколко проверени услуги. Каквито и заявки за услуги да правят потребителите ви, каквито и клиенти и сървъри да инсталират на машините си след това, друг достъп до Internet, освен позволения, няма да получат. Но такова предположение има само временен ефект. Защитната стена, както и всички останали методи за защита, са част от непрекъснати действия за подобряване на сигурността и надеждността на мрежата.

Защитната стена не може да предпазва от вируси

Въпреки че защитната стена сканира входящия трафик, за да определи дали е допустим във вътрешната мрежа, това се отнася предимно за за портовете и за адресите на източника и получателя. Но не се отнася за съдържанието на пренасяните данни и за достъпа на определени процеси до определени мрежови устройства или отдалечени процеси. Откриването на вирус в случаен пакет от данни, минаващ през защитната стена, е много трудно, защото изисква:

- разпознаване, че пакета е част от програма, което е невъзможно в транспортно и мрежово ниво на комуникация;
- определяне, как би трябвало да изглежда програмата и сравняване с това, как изглежда сега;

- ако е налице разлика, вземане на решение, че промяната се дължи именно на вирус.

В този случай са необходимо други програми, които могат да анализират данните, след като са доставени в съответния хост и комуникационния стек не е свързан с тях. Тогава могат да се стартират процеси за анализ на файлове с цел търсене на определени сигнатури в тях или стартиране на анализи за търсене на поредици от системни събития. Такива системи са системите за детектиране на интрузия.

КОНТРОЛНИ ВЪПРОСИ:

1. Каква е разликата между защитна стена и екраниращ рутер?
2. Какви са предимствата на екраниращите рутери пред защитните стени?
3. Напишете поне две различни правила за ограничаване на трафик от сървър предоставящ WWW услуги.
4. Каква защита се постига при използване на две демилитализирани зони спрямо използване на една демилитализирана зона? Аргументирайте отговора си с примери.
5. Дадена фирма има три подмрежи – А, Б и В. Хостовете от мрежа А не трябва да имат достъп до интернет. Хостовете от мрежи Б и В не трябва да имат достъп помежду си. Хостовете от мрежа Б могат да ползват само електронна поща в Интернет от определен от фирмата сървър. Фирмата има IP мрежа от клас С. Трите подмрежи е необходимо да се разделят със защитни стени. Предложете вариант и го обосновете.
6. Какви услуги могат да се разполагат на бастион хостове? Дайте примери.
7. Как може да се ограничи трафик към даден IP адрес при използване на прокси услуга.
8. Защо екраниращият рутер не може да ограничава достъпа на програми до комуникационния стек?