تصميم الشبكات

CECC815

المحاضرة 05

تصميم الشبكات المحلية (LAN) – الجدران النارية

د. أحمد محمود أحمد

المراجع

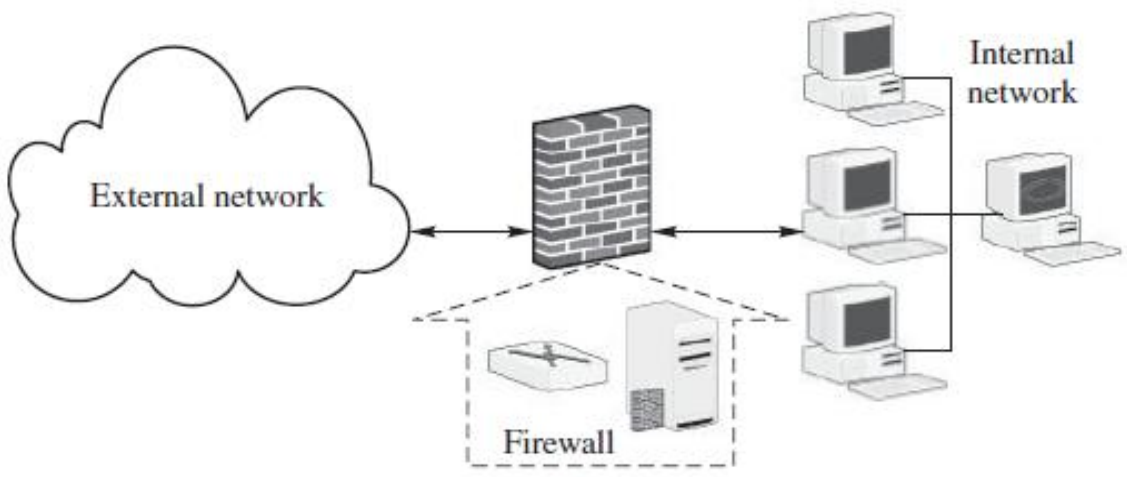
1. Computer Security: Principles and Practice, William Stallings, Lawrie Brown, Pearson, 4th Edition, 2018.

2. Computer networking: a top-down approach. I James F. Kurose, Keith W. Ross, Pearson, 7th Edition, 2017.

مخطط المحاضرة

- الإطار العام للجدار الناري
- خصائص الجدار الناري وسياسة الوصول (Access Policy)
- أنواع الجدران النارية
- الأنظمة الموثوقة والمضيفات الحصينة (Bastion Hosts)
- تكوينات (توليفات) الجدران النارية (Firewall Configurations)
- الجدران النارية في المكاتب الصغيرة والمكاتب المنزلية
- تصنيف آخر لأنواع الجدران النارية
- مسألة

الإطار العام للجدار الناري



Schematic of a firewall

- يُستخدم الجدار الناري كحاجز بين الإنترنت والشبكة الداخلية.
- تُعد الجدران النارية ضرورية لأن خوارزميات التشفير لا تستطيع، بمفردها، منع الحزم الخبيثة بفاعلية من الدخول إلى الشبكة الداخلية.
  - الشبكة الداخلية، هي شبكة تقع تحت سيطرة مالكها.
- قد يكون الجدار الناري جهازًا ماديًا (سريعة لكن صعبة التحديث)، أو حزمة برمجية (بطيئة لكن سهلة التحديث)، أو مزيجًا من الاثنين.

خصائص الجدار الناري وسياسة الوصول (Access Policy)

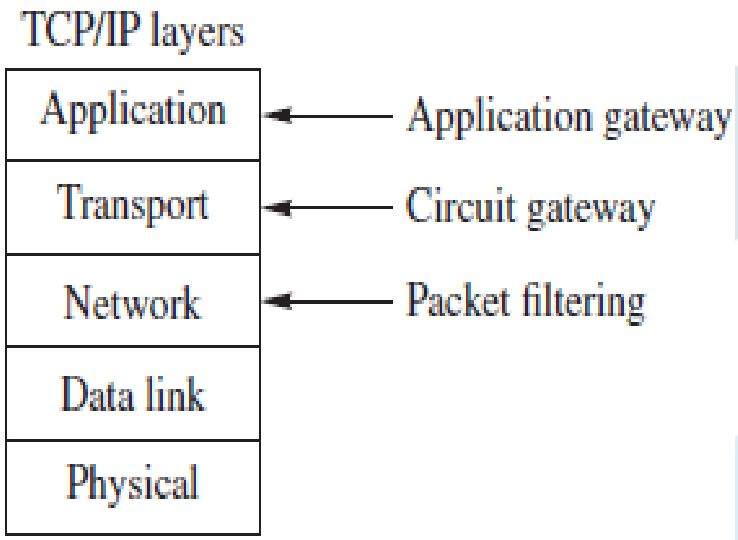
❖ مواصفات الجدار الناري:

- يجب أن تمر جميع حركة البيانات من الداخل إلى الخارج، والعكس، عبر الجدار الناري.
- لا يُسمح بالمرور إلا لحركة البيانات المصرّح بها وفق سياسة الأمن المحلية.
- ينبغي أن يكون الجدار الناري نفسه محصّنًا ضد الاختراق.

❖ يمكن لسياسة الوصول في الجدار الناري أن تستخدم الخصائص الآتية لترشيح حركة البيانات:

- عنوان IP وقيم البروتوكولات.
- بروتوكول التطبيق.
- هوية المستخدم.
- نشاط الشبكة: مثل وقت الاستخدام (ساعات العمل) أو معدل الطلبات.

الإطار العام للجدار الناري



Firewall placements at different layers

❖ يمكن تصنيف الجدار الناري إلى:

- مرشح حزم (Packet filter).
- بوابة دوائر (Circuit gateway).
- بوابة تطبيقات (Application gateway).
- مرشح حزم ديناميكي (DPF Dynamic Packet Filter): وهو نظام يجمع بين مرشح الحزم وبوابة الدوائر.

أنواع الجدران النارية

- **جدار ترشيح الحزم (Packet filtering firewall):** يطبّق مجموعة من القواعد على كل حزمة IP واردة أو صادرة، ثم يمرر الحزمة أو يحجبها بناءً على:
  - عنوان IP المصدر، وعنوان IP الوجهة، وأرقام منافذ المصدروالوجهة، وحقل بروتوكول IP.
- **جدار الفحص ذي الحالة (Stateful Inspection Firewall):** يتشدد في قواعد حركة TCP من خلال **إنشاء سجل** لاتصالات TCP الصادرة. ويخصّص إدخالًا لكل اتصال قائم حاليًا.
- **بوابة مستوى التطبيق (Application-level gateway):** وتُسمى أيضًا وكيل التطبيق (**Application proxy**)، تعمل وسيطًا يمرر حركة البيانات على مستوى التطبيقات.
- **بوابة مستوى الدائرة (Circuit-level gateway):** أو وكيل مستوى الدائرة (**Circuit-level proxy**)، فهي وظيفة متخصصة تنفذها بوابة مستوى التطبيق لبعض التطبيقات.

مرشحات الحزم Packet Filters

- لا يفحص مرشح الحزم إلا ترويسات IP وترويسات TCP (headers).
  - الترشيح الوارد (Ingress filtering): يفحص الحزم الداخلة إلى الشبكة الداخلية من الخارج.
  - الترشيح الصادر (Egress filtering): يفحص الحزم الخارجة من الشبكة الداخلية إلى الخارج.
- يمكن أن يكون ترشيح الحزم على أحد النحوين الآتيين:
  - الترشيح ذو الحالة (Stateful filtering): يفحص حالة اتصالات الشبكة.
    - يسمح الجدار الناري للحزمة بالمرور إذا كانت تنتمي إلى حالة اتصال قائمة، أو إذا كانت طلبًا مشروعًا لإنشاء اتصال. وبخلاف ذلك يحجبها.
  - الترشيح عديم الحالة (Stateless filtering)
- غالبًا ما يُستخدم الترشيح ذو الحالة وعديم الحالة معًا، مع تطبيق الترشيح ذي الحالة أولًا.

مرشحات الحزم: الترشيح عديم الحالة (Stateless filtering)

- يتعامل مع كل حزمة بوصفها كيانًا مستقلًا، ولا يتتبّع الحزم التي عولجت سابقًا.
  - يفحص الحزمة عند وصولها ويتخذ قرارًا من دون ترك أي سجل في الرزمة من دون فحص.
- يستخدم مجموعة من القواعد تُعرف باسم قائمة التحكم في الوصول (ACL) من أجل:
  - غالبًا: فحص عنوان IP المصدروعنوان IP الوجهة في ترويسة IP.
  - وقد يفحص: منفذ المصدرومنفذ الوجهة في ترويسة TCP أو ترويسة UDP.
- إذا كان عنوان IP أو منفذ TCP/UDP غير موثوق أو غير مرغوب فيه، فيتم حظره.

مرشحات الحزم: الترشيح عديم الحالة (Stateless filtering)

- تُفحص القواعد في قائمة ACL قاعدةً تلو الأخرى من الأعلى إلى الأسفل.
  - إذا لم تتضمن قائمة ACL قاعدة لمعالجة الحزمة قيد الفحص؛ كأن لا يظهر عنوان IP أو المنفذ الخاص بها في القائمة، فإن هذه الحزمة تُحجب افتراضيًا.
  - وفي نهاية قائمة ACL النموذجية توجد قاعدة افتراضية تحجب كل الحزم.
  - تُحجب الحزمة الواردة إذا كان عنوان المصدر فيها عنوانًا داخليًا، لأن ذلك يُعد مؤشر هجوم.
  - وتُحجب أي حزمة، واردة كانت أو صادرة، إذا حددت الموجّهات التي ينبغي استخدامها، لأن ذلك يُعد مؤشر هجوم.

مرشحات الحزم: الترشيح عديم الحالة (Stateless filtering)

Sample ACL rules for ingress filtering, where "int" represents "internal," "ext" represents "external," and "addr" represents "address"

int addr	int port	ext addr	ext port	Action	Comment
*	*	a.b.c.d	*	Block	Block packets from this IP address
192.63.8.254	110	*	*	Allow	Open internal POP3 port

Sample ACL rules for egress filtering

int addr	int port	ext addr	ext port	Action	Comment
*	*	a.b.c.d	*	Block	Block packets to this IP address
*	*	*	25	Allow	Allow packets to external SMTP port
*	*	*	> 1023	Allow	Allow packets to nonstandard port

The default rule at the end of ACL

int addr	int port	ext addr	ext port	Action	Comment
*	*	*	*	Block	ACL default rule: block everything

يرمز a.b.c.d إلى عنوان IP.
ويرمز * إلى أي عنوان أو أي منفذ.

مرشحات الحزم: الترشيح ذو الحالة (Stateful Filtering)

- يُشار إليه أيضًا بترشيح حالة الاتصال.
  - وهو يتتبّع الاتصالات بين مضيف داخلي ومضيف خارجي.
    - توضح حالة الاتصال ما إذا كان الاتصال من نوع TCP أو UDP، وما إذا كان الاتصال قائمًا بالفعل.
- تُخزّن حالات الاتصال في جدول للحالات.
  - عند وصول حزمة، واردة كانت أو صادرة، يتحقق الجدار الناري مما إذا كانت الحزمة تنتمي إلى اتصال قائم في جدول الحالات.
    - إذا كان الأمر كذلك، يسمح الجدار الناري بمرور الحزمة ويحفظ معلوماتها، مثل رقم تسلسل TCP، لاستخدامها لاحقًا.
    - أما إذا كانت الحزمة من نوع SYN، فينشئ إدخالًا جديدًا في جدول الحالات.
    - وفي غير ذلك، يتخلص الجدار الناري من الحزمة.

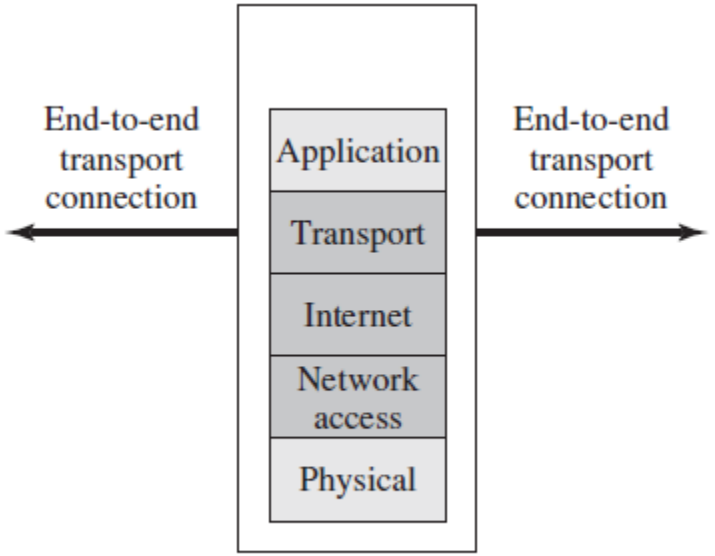
مرشحات الحزم: الترشيح ذو الحالة (Stateful Filtering)

Example of connection state table

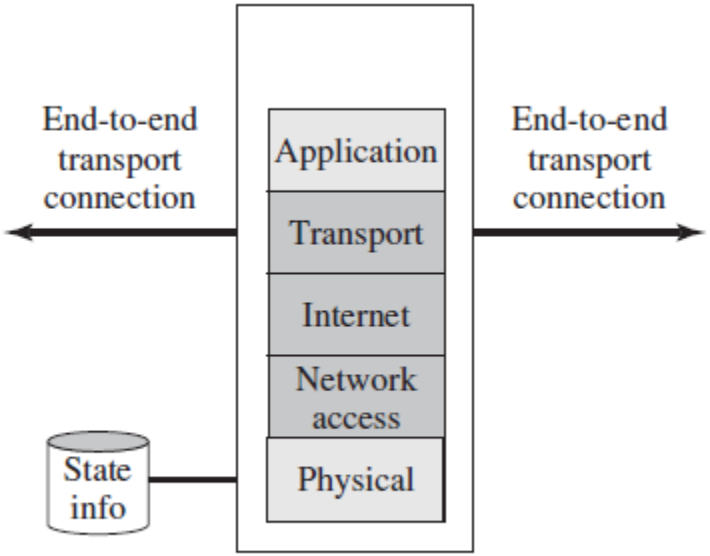
Client addr	Client port	Server addr	Server port	Connection state	Protocol
219.22.101.32	1030	129.63.24.84	25	Established	TCP
219.22.101.54	1034	129.63.24.84	161	Established	UDP
210.99.201.14	2001	129.63.24.87	80	Established	TCP
24.102.129.21	3389	129.63.24.87	110	Established	TCP

نفترض أن الموجّهات تتضمن مرشحات حزم مدمجة (built-in packet filters).

مرشحات الحزم (Packet Filters)



Packet filtering firewall



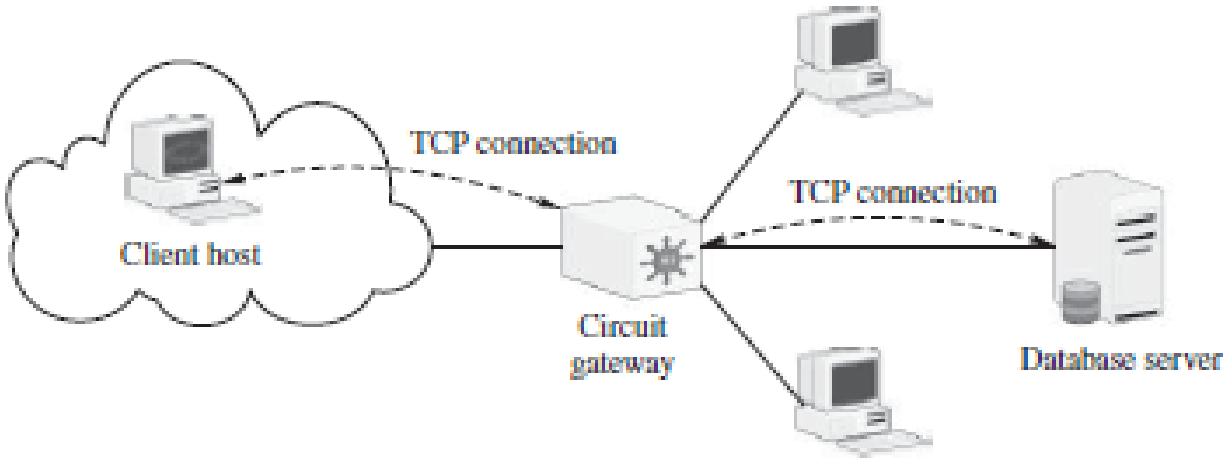
Stateful inspection firewall

بوابات الدوائر (Circuit Gateways): البنى الأساسية

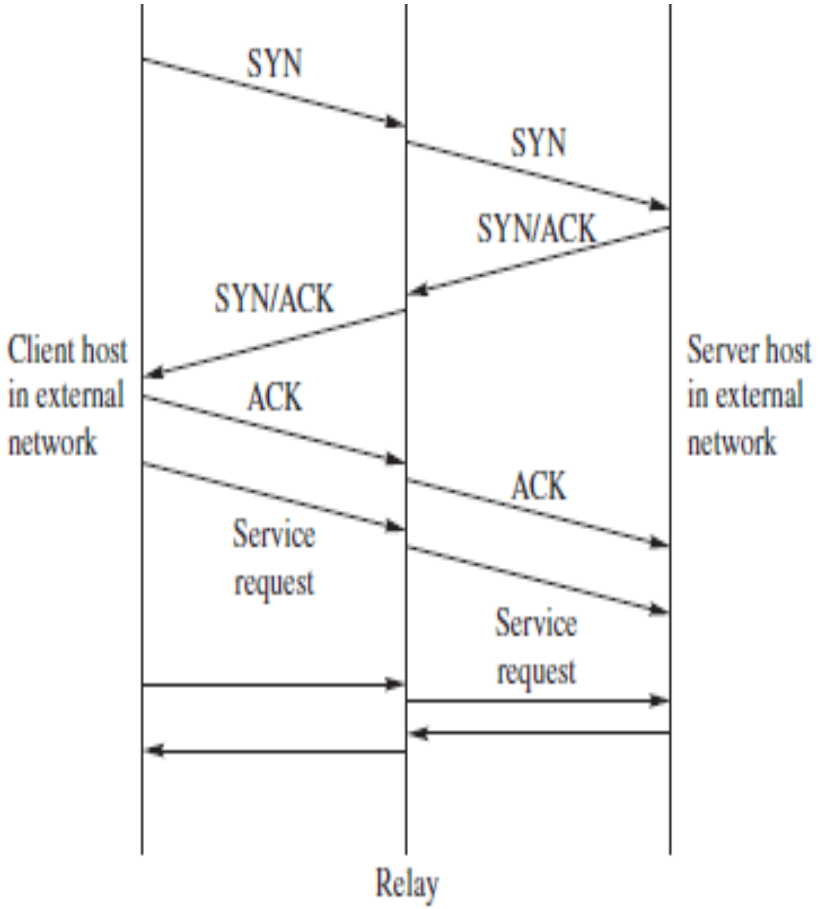
- تُعرف أيضًا باسم بوابات مستوى الدائرة (Circuit-level gateways) أو جدران الوكيل الشفافة (Transparent proxy firewalls)، وتعمل في طبقة النقل.
  - تقيّم المعلومات المتعلقة بعناوين IP وأرقام المنافذ الواردة في ترويسات TCP أو UDP.
- تهدف بوابة الدائرة إلى توصيل (Relay) اتصال TCP بين مضيف داخلي ومضيف خارجي.

1. تتحقق بوابة الدائرة أولًا من صلاحية جلسة TCP أو UDP.
2. ثم تنشئ اتصالًا مستقلًا مع المضيف الداخلي و اتصالًا آخر مع المضيف الخارجي.
3. وتحتفظ بجدول للاتصالات الصالحة، وتقارن الحزم الواردة بالمعلومات الموجودة في ذلك الجدول.
4. وعند انتهاء الجلسة، يُزال الإدخال المقابل لها.

بوابات الدوائر(Circuit Gateways): البنى الأساسية



Schematic of a circuit gateway



بوابات الدوائر (Circuit Gateways): SOCKS

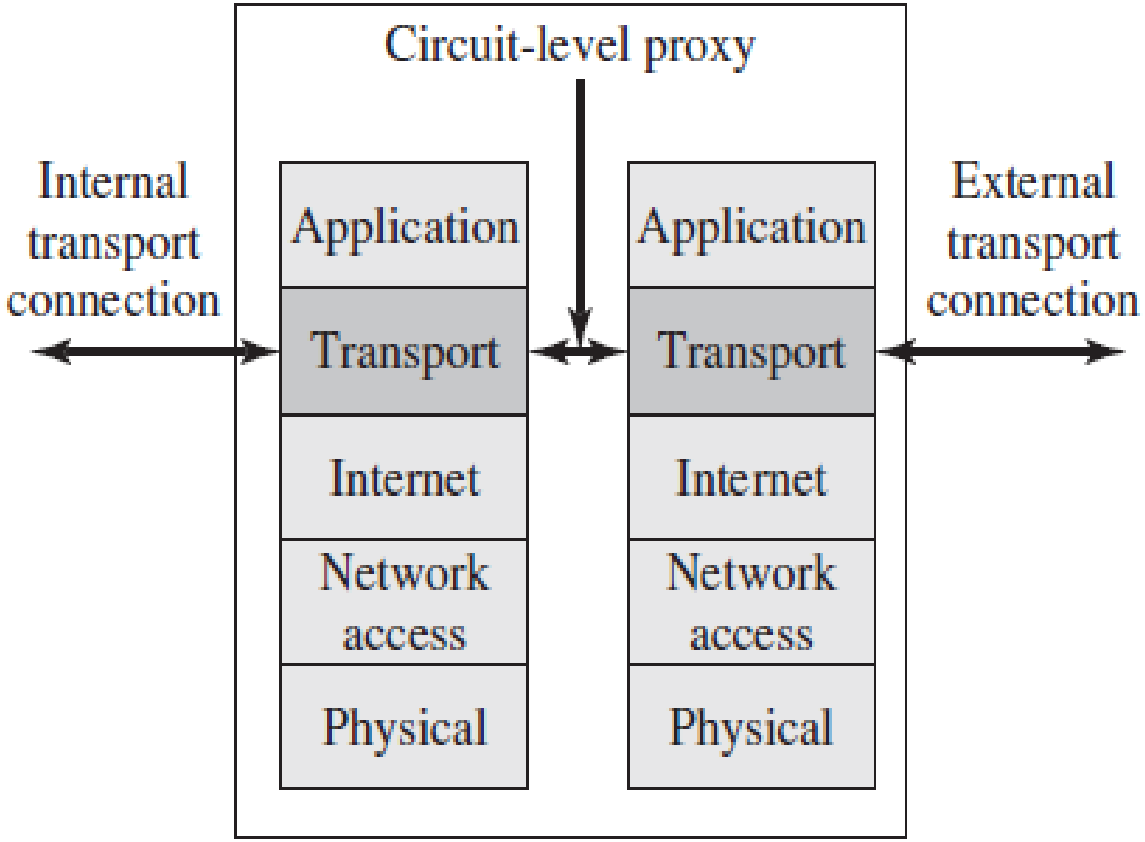
- SOCKS، اختصارًا لـ SOCKetS، هو بروتوكول شبكي يُستخدم لتنفيذ بوابات الدوائر.
- يتكون SOCKS من ثلاثة مكوّنات:
  - خادم SOCKS: يعمل على جدار ناري لترشيح الحزم عبر المنفذ 1080.
  - عميل SOCKS: يعمل على مضيف عميل خارجي.
  - مكتبة عميل SOCKS (library): تعمل على مضيف داخلي.

بوابات الدوائر (Circuit Gateways): SOCKS

❖ عندما يريد عميل خارجي الحصول على خدمة من خادم داخلي محمي بواسطة SOCKS:

- يجب على العميل أولًا إنشاء اتصال TCP مع خادم SOCKS.
- بعد ذلك يتفاوض مع خادم SOCKS لاختيار خوارزمية المصادقة، ثم يقدّم معلومات المصادقة ويرسل طلب الترحيل (Relay request).
- يتحقق خادم SOCKS من معلومات المصادقة المقدمة، ثم يقرر ما إذا كان سينشئ اتصال ترحيل (Relay connection) مع الخادم الداخلي كما طُلب.
- حتى إذا كان العميل الخارجي يريد فقط إرسال حزمة UDP إلى مضيف داخلي، فإنه لا يزال بحاجة إلى إنشاء اتصال TCP مع خادم SOCKS وتقديم معلومات المصادقة.

بوابات الدوائر (Circuit Gateways)



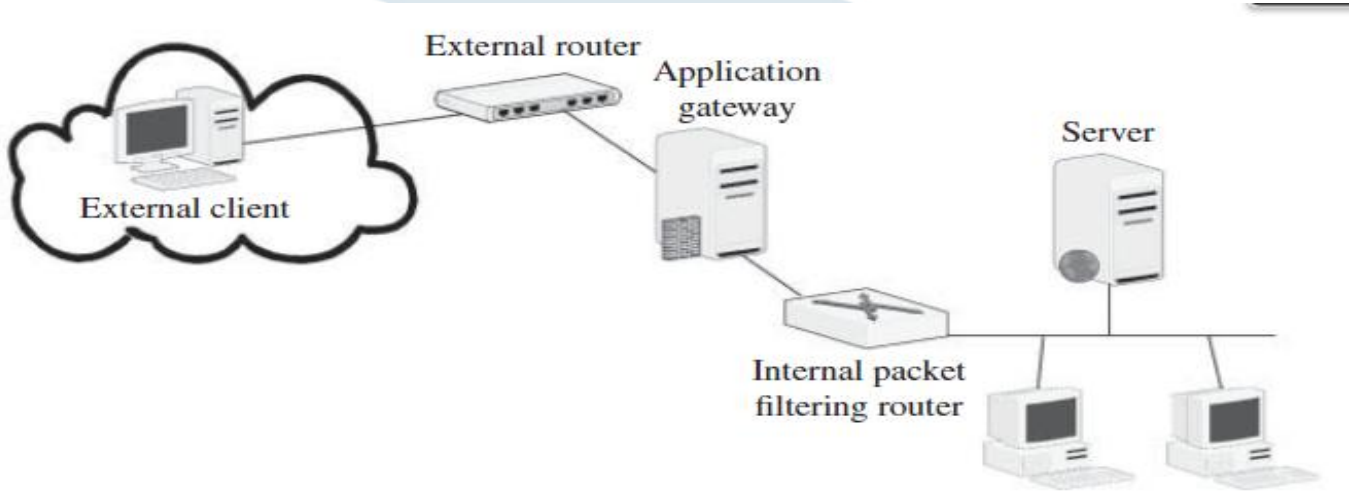
Circuit-level proxy firewall

بوابات التطبيقات (Application Gateways)

- تُعرف أيضًا باسم بوابات مستوى التطبيق (Application-Level Gateways) (ALG) أو خوادم الوكيل (Proxy servers).
  - وهي حزم برمجية تُثبّت على حاسوب مخصص.
- تجري بوابة مستوى التطبيق فحصًا عميقًا لكل حزمة IP، سواء كانت واردة أم صادرة.
  - تفحص صيغ برامج التطبيقات الموجودة داخل الحزمة، مثل صيغة MIME وصيغة SQL، وتتحقق مما إذا كانت الحمولة مسموحًا بها.
    - وقد تتمكن من كشف فيروس حاسوبي داخل الحمولة.
    - كما قد تتمكن من كشف الشيفرات الخبيثة وعزل الحزم المشبوهة، إضافة إلى حجب الحزم ذات عناوين IP أو منافذ TCP المشبوهة.

بوابات التطبيقات: بوابات التخزين المؤقت (Cache Gateways)

- تُستخدم **لحماية خادم الويب من الاختراق**، إذ تعمل وكيلًا لخادم الويب وتُسمى **خادم وكيل الويب** (Web Proxy Server)، حيث تُجري فحصًا عميقًا للحزم قبل تمريرها إلى خادم الويب.
- يفحص خادم وكيل الويب أيضًا صفحات الويب التي يرسلها خادم الويب إلى العميل الخارجي ويخزنها في ذاكرته المخبئية؛ وتُسمى هذه الحالة **بوابات التخزين المؤقت**.
- غالبًا ما تُستخدم بوابة التطبيق مع موجّه لترشيح الحزم، بحيث يوضع الموجّه خلف البوابة.

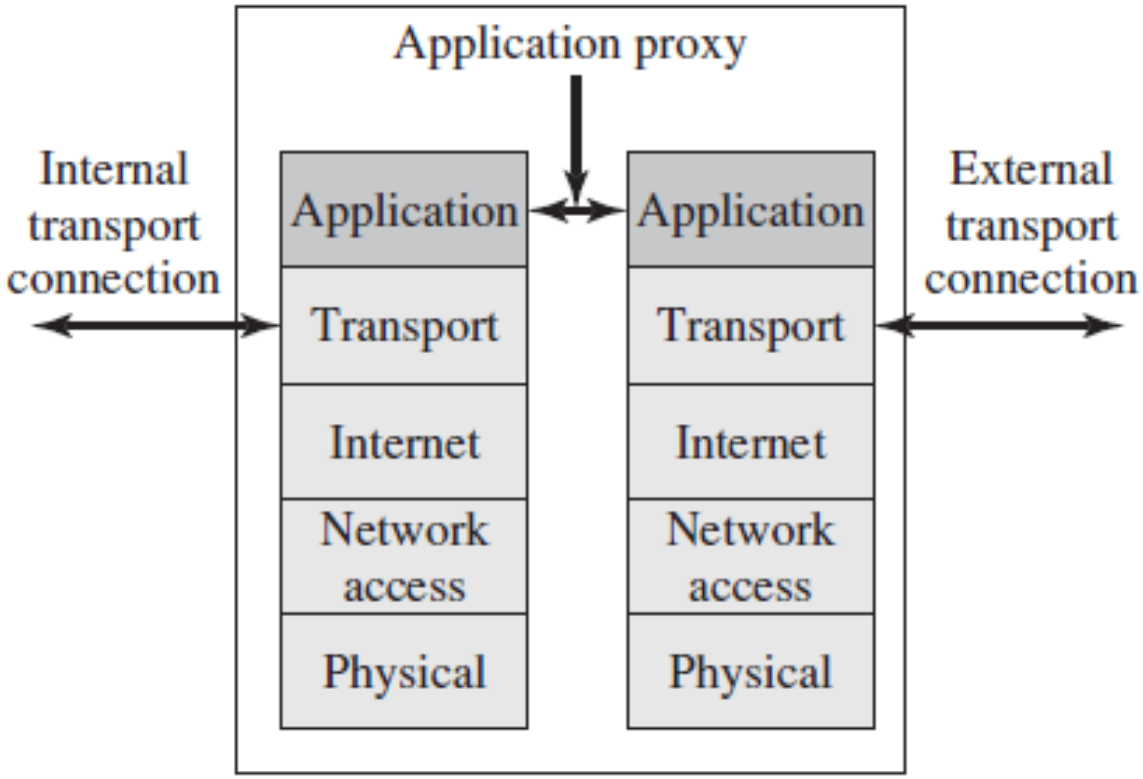


Schematic of an application gateway

بوابات التطبيقات (Application Gateways): الفحص ذو الحالة للحزم

- يوسّع الفحص ذو الحالة للحزم (Stateful Packet Inspection) (SPI) مفهوم ترشيح الحزم ذي الحالة (Stateful Packet Filtering) (SPF) ليشمل فحص حمولة الحزمة أيضًا.
- يفحص SPI ما إذا كان:
  - الحزمة تنتمي إلى اتصال مشروع.
  - تنسيق محتواها يتوافق مع نوع الخدمة التي صُمم الاتصال لتقديمها.

بوابات التطبيقات (Application Gateways)



Application proxy firewall

الأنظمة الموثوقة والمضيفات الحصينة (Bastion Hosts)

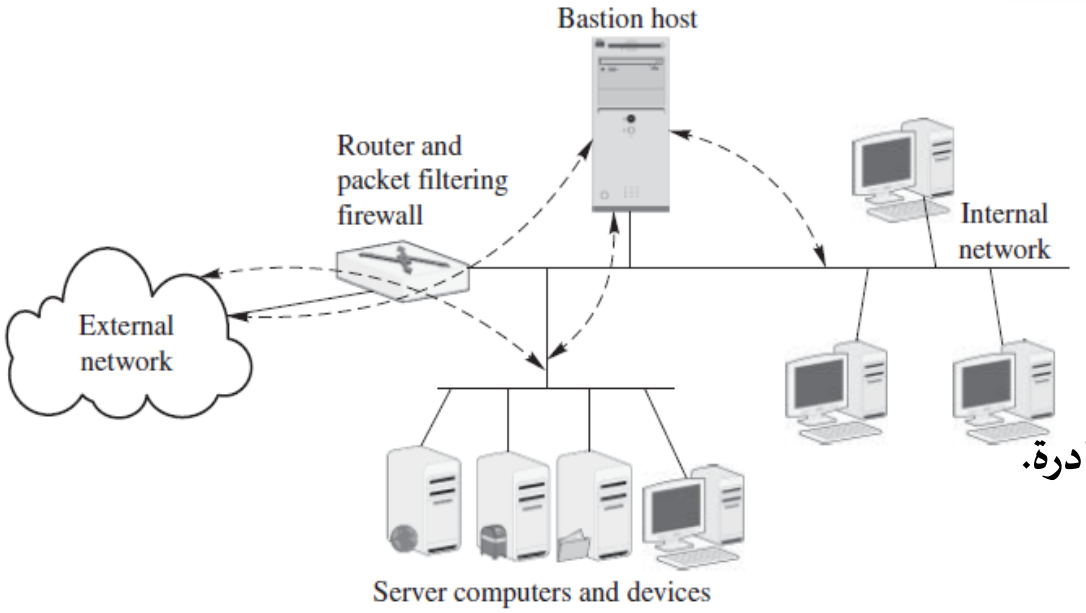
- تحتاج حواسيب البوابات (Gateway computers) إلى مستويات أقوى من الحماية الأمنية.
  - هناك إجراءان شائعان:
    - جعل نظام التشغيل نظامًا موثوقًا.
    - تهيئة حواسيب البوابات لتعمل كمضيفات حصينة.
- المضيفات الحصينة هي حواسيب مزودة بآليات دفاع قوية.
  - وغالبًا ما تعمل حواسيب مضيفة لتنفيذ بوابات التطبيقات، وبوابات الدوائر، وأنواع أخرى من الجدران النارية.
  - ولا تُثبّت على المضيف الحصين إلا تطبيقات الشبكات الضرورية تمامًا، مثل SSH وDNS وSMTP وبرامج المصادقة.
  - وغالبًا ما تُستخدم البوابات العاملة على مضيف حصين مع مرشحات الحزم.

تكوينات (توليفات) الجدران النارية (Firewall Configurations)

- توجد عدة تكوينات (توليفات) شائعة للجدران النارية:
  - نظام المضيف الحصين أحادي الواجهة (Single-homed bastion host system) (SHBH).
  - نظام المضيف الحصين ثنائي الواجهة (dual-homed bastion host system) (DHBH).
  - الشبكات الفرعية المحجوبة، أو المناطق منزوعة السلاح (demilitarized zones) (DMZ).

تكوينات الجدران النارية: SHBH

- يتكون من موجّه لترشيح الحزم (A packet-filtering router) ومضيف حصين (Bastion host):
  - يربط الموجّه الشبكة الداخلية بالشبكات الخارجية.
  - يقع المضيف الحصين داخل الشبكة الداخلية.
- يفحص الموجّه الحزمة الواردة (Ingress packet).
  - إذا اجتازت الحزمة الفحص، يمررها الموجّه إلى المضيف الحصين.
- تمر الحزم الصادرة (Egress packets) عبر المضيف الحصين.
  - يفحص جدار ترشيح الحزم (Packet filtering firewall) كل حزمة صادرة.
  - ويحجبها إذا:
    - لم يكن عنوان مصدرها هو عنوان IP الخاص بالمضيف الحصين.
    - أو إذا أخفقت في قواعد الترشيح الأخرى.

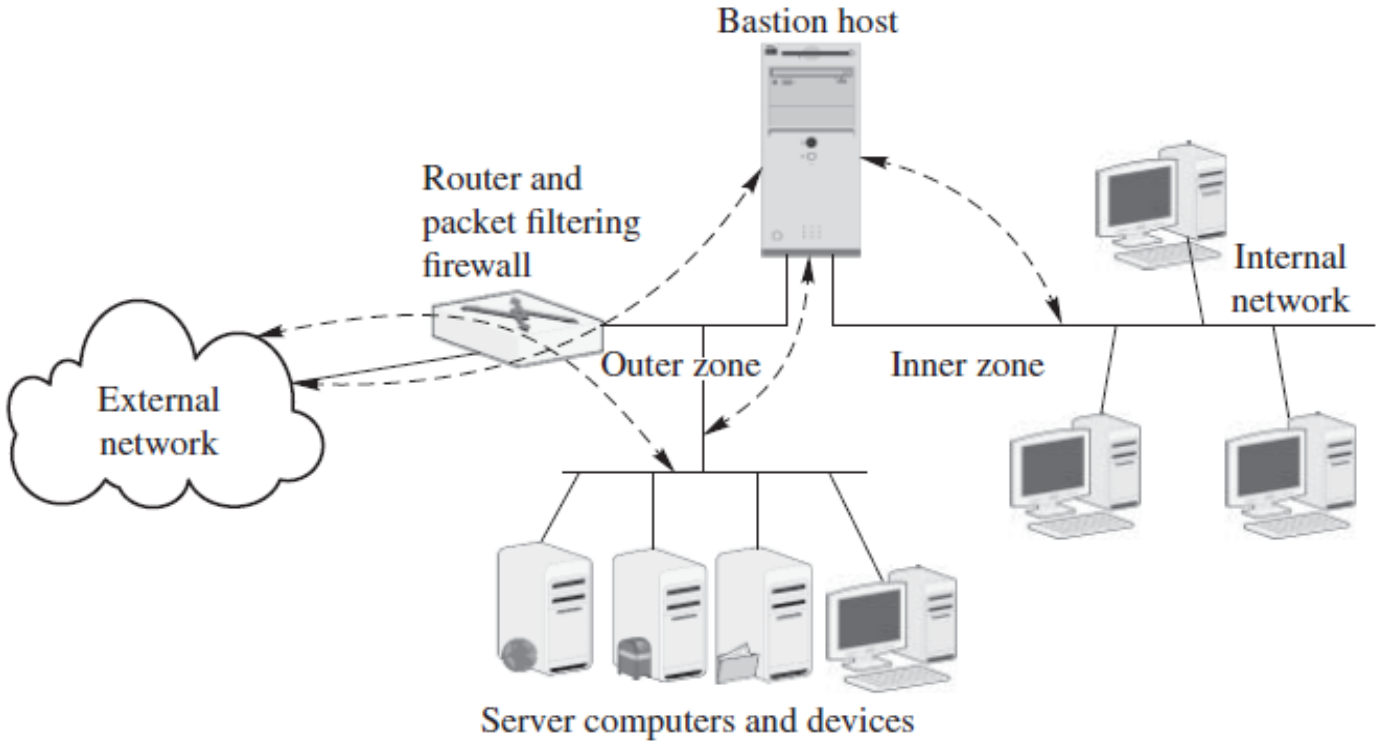


Schematic of a single-homed bastion host network, where the dotted arrow lines show the actual communications and the solid lines show the physical network connections

تكوينات الجدران النارية: DHBH

- تقسم شبكة DHBH الشبكة الداخلية إلى منطقتين:
  - المنطقة الداخلية، أو المنطقة الخاصة (Inner zone (the private zone): لا يمكن الوصول إلى عناوين IP الخاصة بحواسيب المضيف في المنطقة الخاصة، من الشبكة الخارجية.
  - المنطقة الخارجية (Outer zone): قد تكون عناوين IP الخاصة بحواسيب المضيف في المنطقة الخارجية قابلة للوصول مباشرة من الإنترنت.
- يوضع الموجّه بين الشبكة الخارجية والمنطقة الخارجية، وكذلك بين الشبكة الخارجية والمضيف الحصين.
  - أما المنطقة الداخلية في DHBH فلا تتصل إلا بالمضيف الحصين.
    - تُحمى حواسيب المضيف (Host computers) في المنطقة الداخلية بكلٍّ من المضيف الحصين وموجّه ترشيح الحزم.
    - وتُحمى أجهزة الخوادم في المنطقة الخارجية بواسطة موجّه ترشيح الحزم.
- تتيح DHBH لخوادم المنطقة الخارجية الاتصال بالإنترنت من دون المرور عبر المضيف الحصين.

تكوينات الجدران النارية: DHBH

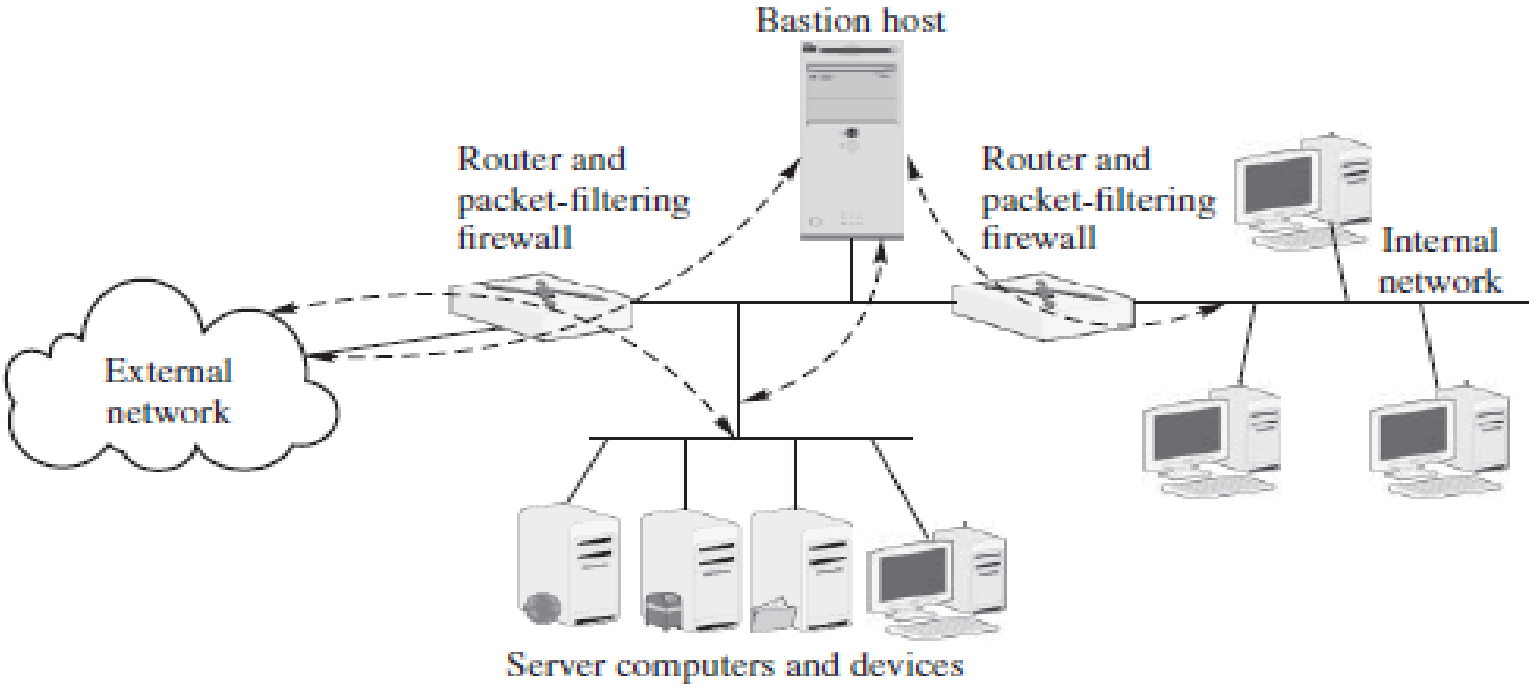


Schematic of a dual-homed bastion host network, where the dotted arrow lines show the actual communications and the solid lines show the physical network connections

تكوينات الجدران النارية: الشبكات الفرعية المحجوبة أو المناطق منزوعة السلاح

- تُعد من أكثر تكوينات الجدران النارية أمانًا.
- تتكون الشبكة الفرعية المحجوبة من مضيف حصين وموجّهين لترشيح الحزم.
  - وهي تشبه شبكة SHBH مع إضافة موجّه ثانٍ لترشيح الحزم بين المضيف الحصين والشبكة الداخلية.
  - ينشئ الجداران الناريان لترشيح الحزم (Packet-filtering firewalls) شبكة فرعية معزولة ومحجوبة بينهما.
  - ولا تستطيع المضيفات الداخلية الاتصال بالمضيفات الخارجية إلا عبر الخوادم أو الأجهزة الموجودة في الشبكة الفرعية المحجوبة (screened subnetwork).

تكوينات الجدران النارية: الشبكات الفرعية المحجوبة



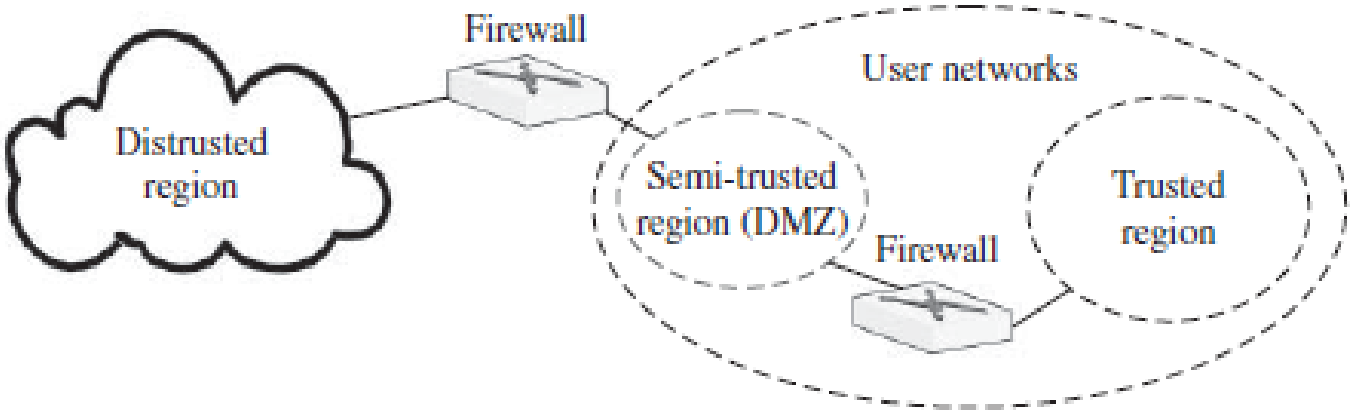
Schematic of a screened subnet system, where the dotted arrow lines show the actual communications and the solid lines show the physical network connections

تكوينات الجدران النارية: المناطق منزوعة السلاح DMZ

- المنطقة منزوعة السلاح (DMZ): هي الشبكة الفرعية الو اقعة بين جدارين ناريين داخل الشبكة الداخلية.
  - يحمي الجدار الناري الخارجي شبكة DMZ الفرعية من الشبكات الخارجية،
  - بينما يحمي الجدار الناري الداخلي الشبكة الداخلية من DMZ.
  - وقد تحتوي شبكة DMZ الفرعية على مضيف حصين أو لا تحتوي عليه.
- يمكن تعميم مفهوم DMZ أحادية الطبقة إلى DMZ متعددة الطبقات، حيث قد تحتوي DMZ على DMZ فرعية.

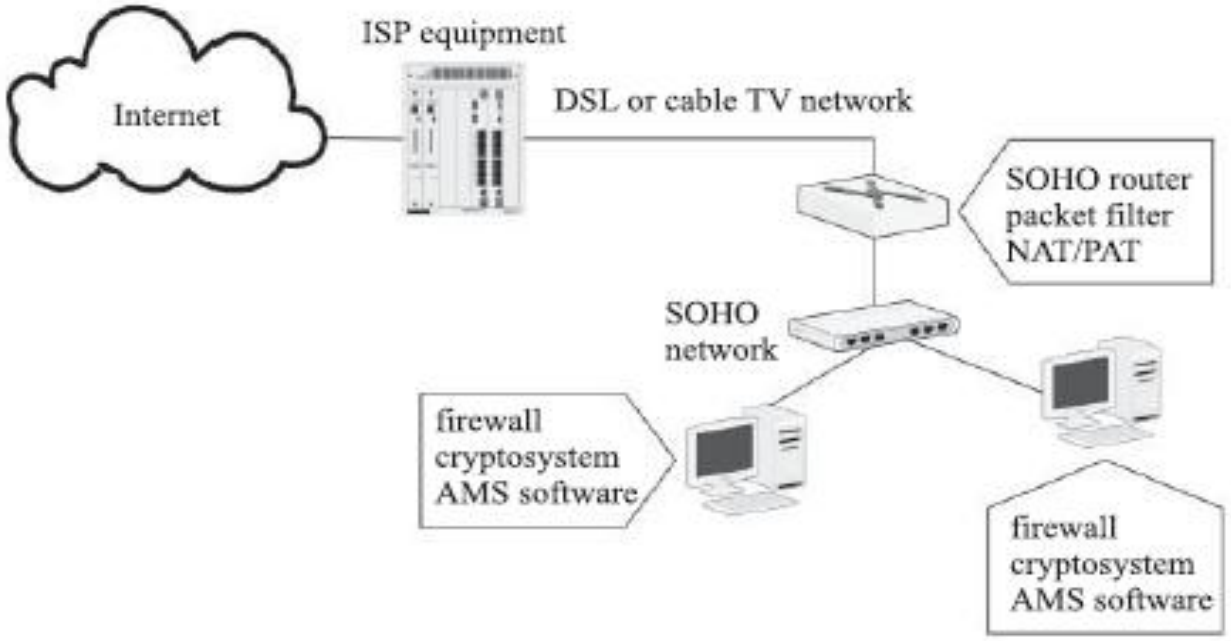
تكوينات الجدران النارية: طوبولوجيا أمن الشبكات

- يمكن استخدام الجدران النارية لتقسيم الشبكات إلى ثلاث مناطق منفصلة: منطقة غير موثوقة، ومنطقة شبه موثوقة، ومنطقة موثوقة.



A schematic of network security topology

جدران المكاتب الصغيرة والمكاتب المنزلية النارية



Schematic of a SOHO firewall network

- يدعم الموجّه المستخدم في الاتصال عادةً تقنيتي NAT/PAT وترشيح الحزم.
- ويُشار إلى مثل هذا الموجّه أحيانًا باسم جدار SOHO الناري.

SOHO: Small Office/Home Office

تصنيف آخر لأنواع الجدران النارية

- الجدران النارية المعتمدة على المضيف (Host-Based Firewalls).
- جدار ناري لجهاز الشبكة (Network Device Firewall).
- الجدار الناري الافتراضي (Virtual Firewall).
- الجدار الناري الشخصي (Personal Firewall).

مسألة (1)

❖ السؤال:

- اشرح كيف يمكن تصميم شبكة باستخدام DMZ لمؤسسة تمتلك خوادم عامة مثل Web Server وMail Server وDNS Server و VPN Server، مع وجود أنظمة داخلية حساسة مثل قواعد البيانات و أنظمة الموظفين. وضّح أماكن وضع الخوادم، وقواعد الجدار الناري المناسبة، وقارن بين Single Firewall DMZ وDual Firewall DMZ مع اختيار التصميم الأفضل.

❖ الجواب:

- تُعد DMZ منطقة عازلة تُستخدم لوضع الخوادم التي يجب أن تكون متاحة من الإنترنت، وذلك لحماية الشبكة الداخلية من الوصول المباشر. في هذا التصميم يتم تقسيم الشبكة إلى ثلاث مناطق: الإنترنت، وDMZ، والشبكة الداخلية.
- توزيع الخوادم:
  - توضع داخل DMZ الخوادم العامة التالية: WEB, MAIL, DNS, VPN servers
  - أما داخل الشبكة الداخلية فتوضع الأنظمة الحساسة التالية: (Database, HR, Students) servers, Hosts

مسألة (1)

❖ السؤال:

- اشرح كيف يمكن تصميم شبكة باستخدام DMZ لمؤسسة تمتلك خوادم عامة مثل Web Server وMail Server وDNS Server و VPN Server، مع وجود أنظمة داخلية حساسة مثل قواعد البيانات و أنظمة الموظفين. وضّح أماكن وضع الخوادم، وقواعد الجدار الناري المناسبة، وقارن بين Single Firewall DMZ وDual Firewall DMZ مع اختيار التصميم الأفضل.

❖ الجواب:

- التبرير الأمني:

  - الخوادم العامة تحتاج إلى استقبال طلبات من الإنترنت، بينما الأنظمة الداخلية يجب أن تبقى معزولة وآمنة ولا تكون مرئية للعالم الخارجي بصورة مباشرة.

مسألة (1)

❖ تكملة الجواب:

- قواعد الجدار الناري :يجب السماح فقط بالخدمات الضرورية من الإنترنت إلى DMZ، مثل:
  - HTTP وHTTPS إلى Web Server
  - SMTP إلى Mail Server
  - استعلامات DNS إلى DNS Server
  - اتصالات VPN إلى VPN Server.

وفي المقابل يجب منع أي اتصال مباشر من الإنترنت إلى الشبكة الداخلية، مع تقييد الاتصال بين DMZ والشبكة الداخلية ليكون فقط عند الحاجة وبمنافذ محددة جدًا.

مسألة (1)

❖ تكملة الجواب:

- حماية قاعدة البيانات: إذا احتاج الموقع الإلكتروني إلى البيانات من قاعدة البيانات، فمن الأفضل ألا يتصل Web Server مباشرة بقاعدة البيانات، بل يمر عبر Application Server أو API داخلي. هذا الأسلوب يقلل المخاطر، ويمنع كشف قاعدة البيانات مباشرة، ويرفع مستوى التحكم في الصلاحيات والمراقبة.
- المقارنة بين التصميمين:

التصميم	المزايا	العيوب
Single Firewall DMZ	أقل تكلفة وأسهل في الإدارة	نقطة فشل واحدة ومستوى العزل أقل
Dual Firewall DMZ	عزل أمني أقوى وحماية أفضل للأنظمة الداخلية	تكلفة أعلى وإدارة أكثر تعقيدًا

- الاختيار الأنسب: التصميم الأنسب لهذه المؤسسة هو Dual Firewall DMZ لأنه يوفّر حماية أفضل للبيانات الحساسة، ويمنع انتقال الهجوم بسهولة إلى الشبكة الداخلية مقارنةً بالتصميم ذي الجدار الناري الواحد.

مسألة (1)

❖ تكملة الجواب:

- الخلاصة:

  - وضع الخوادم العامة داخل DMZ لأنها تحتاج إلى الوصول من الإنترنت.
  - إبقاء قواعد البيانات والأنظمة الحساسة داخل الشبكة الداخلية.
  - منع الاتصال المباشر من الإنترنت إلى الشبكة الداخلية.
  - تقييد الاتصال بين DMZ وInternal LAN ليكون فقط عند الحاجة وبمنافذ محددة.
  - اعتماد Dual Firewall DMZ عند وجود بيانات حساسة داخل المؤسسة.

شكراً لحسن الاستماع .... هل من أسئلة؟