مسألة (2)

لدى جامعة خاصة شبكة داخلية تحتوي على الأنظمة التالية:

- شبكة إدارية تضم قواعد بيانات شؤون الطلاب والموظفين.
- شبكة أكاديمية تضم أنظمة التعلم الإلكتروني.
- شبكة مستخدمين داخلية لأعضاء هيئة التدريس والموظفين.
- اتصال إنترنت خارجي للمستخدمين والزوار.

تريد الجامعة نشر الخدمات التالية لتكون متاحة من الإنترنت:

- Web Server للموقع الرسمي للجامعة .
- Mail Server للبريد الإلكتروني.
- DNS Server عام.
- VPN Server للموظفين الذين يعملون عن بعد.

لكن الجامعة تريد في الوقت نفسه حماية الشبكة الداخلية الحساسة، خاصة قواعد البيانات والأنظمة الإدارية، ومنع أي وصول مباشر إليها من الإنترنت.

المطلوب

صمم بنية شبكة تعتمد على DMZ بحيث تحقق المتطلبات التالية :

1. فصل الخوادم العامة المعرضة للإنترنت عن الشبكة الداخلية.
2. السماح للمستخدمين من الإنترنت بالوصول فقط إلى الخدمات العامة المصرّح بها.
3. منع أي اتصال مباشر من الإنترنت إلى الشبكة الداخلية .
4. السماح فقط باتصالات محددة وآمنة بين خوادم DMZ وبعض الأنظمة الداخلية عند الحاجة.
5. توفير سياسات جدار ناري مناسبة بين:
   - الإنترنت و DMZ
   - والشبكة الداخلية DMZ
   - الإنترنت والشبكة الداخلية
6. مراعاة الجوانب الأمنية التالية:
   - مبدأ أقل صلاحية
   - تسجيل ومراقبة الأحداث
   - الحماية من الحركة الجانبية في حال اختراق أحد خوادم DMZ

<u>المطلوب في الحل:</u>

1. رسم مخطط منطقي للشبكة
2. تحديد مكان كل من:
   - Firewall
   - DMZ
   - Internal LAN
   - Public Servers
3. اقتراح قواعد وصول أساسية ACL / Firewall Rules
4. شرح سبب وضع كل خدمة داخل DMZ أو داخل الشبكة الداخلية
5. توضيح كيف يتم حماية قاعدة البيانات الداخلية إذا كان الموقع الإلكتروني يحتاج إلى جلب بيانات منها
6. ما الفرق بين:
   - Single Firewall DMZ
   - Dual Firewall DMZ

   وأيهما أنسب لهذه الجامعة؟ مع التبرير

<u>الحل:</u>

الـ DMZ هي منطقة معزولة توضع فيها الخوادم التي يجب أن تكون متاحة من الإنترنت، بحيث إذا تم اختراق أحد هذه الخوادم لا ينتقل المهاجم مباشرة إلى الشبكة الداخلية. بالتالي نقسم الشبكة إلى ثلاث مناطق رئيسية:

- External Network : الإنترنت.
- DMZ: الخوادم العامة.
- Internal LAN: الأنظمة الحساسة الداخلية

التصميم المقترح:

- **المخطط المنطقي**

```
                Internet
                    |
            [External Firewall]
                    |
        ----------------------------
        |                          |
      DMZ                   [Internal Firewall]
        |                          |
  ------------------               |
  |   |    |    |                 |
Web Mail DNS  VPN              Internal LAN
Server Server Server Server        |
                                   |
                     -------------------------------
                     |             |              |
                Student DB     HR System     Staff PCs
```

- **توزيع الخوادم:**

توضع في DMZ:

- ✓ Web Server
- ✓ Mail Server
- ✓ Public DNS Server
- ✓ VPN Server

توضع داخل الشبكة الداخلية

- ✓ Database Server
- ✓ HR System
- ✓ أجهزة الموظفين
- ✓ الأنظمة التعليمية الداخلية غير العامة

السبب

الخدمات الموجودة في DMZ تحتاج أن تكون متاحة من الإنترنت، لذلك توضع في منطقة شبه معزولة. أما قواعد البيانات والأنظمة الحساسة فلا يجب أن تكون مكشوفة للعالم الخارجي، لذا تبقى داخل الشبكة الداخلية فقط.

- **قواعد الجدار الناري المقترحة**

1. بين الإنترنت و DMZ:

يسمح فقط بالاتصالات الضرورية

- السماح بـ HTTP/HTTPS من الإنترنت إلى Web Server
  - TCP 80, 443
- السماح بـ SMTP إلى Mail Server
  - TCP 25

- السماح بـ DNS queries إلى DNS Server
  - UDP/TCP 53
- السماح بـ VPN إلى VPN Server
  - حسب البروتوكول المستخدم مثل:
    - 4500، 500 UDP لـ IPsec.
    - أو 443 TCP لـ SSL VPN

منع

- أي منفذ آخر غير مصرح به.
- أي وصول مباشر من الإنترنت إلى Internal LAN.

2. بين الإنترنت والشبكة الداخلية:

منع كامل لأي اتصال مباشر من الإنترنت إلى:

- قواعد البيانات
- أجهزة الموظفين
- الأنظمة الإدارية
- الأنظمة التعليمية الداخلية

3. بين DMZ والشبكة الداخلية

السماح فقط بما يلي عند الحاجة:

- Web Server في DMZ يتصل بتطبيق داخلي أو API داخلي محدد فقط.
- Mail Server يتصل بخادم بريد داخلي إن وجد
- VPN Server يسمح للمستخدمين المصرح لهم فقط بالوصول إلى موارد داخلية محددة
- DNS Server يمكنه الاستعلام من DNS داخلي إذا كان التصميم يتطلب ذلك

مثال

إذا كان الموقع الإلكتروني يحتاج بيانات من قاعدة البيانات الداخلية:

- لا نسمح لأي جهاز من DMZ بالوصول المفتوح إلى قاعدة البيانات
- نسمح فقط لـ Web Server أو Application Server بالاتصال إلى DB Server.
- على منفذ قاعدة البيانات فقط:
  - TCP 3306 لـ MySQL .

- TCP 5432 لـ PostgreSQL.
- TCP 1433 لـ SQL Server .

- مع تقييد عنوان المصدر والوجهة بدقة

- **نموذج قواعد ACL / Firewall Rules**

<u>من Internet إلى DMZ</u>

1. Allow Internet ⟶ Web Server : TCP 80,443
2. Allow Internet ⟶ Mail Server : TCP 25
3. Allow Internet ⟶ DNS Server : UDP/TCP 53
4. Allow Internet ⟶ VPN Server : VPN Ports
5. Deny Any ⟶ DMZ Any Other Traffic

<u>من Internet الى Internal LAN</u>

6. Deny Internet ⟶ Internal LAN : Any

<u>من DMZ الى Internal LAN</u>

7. Allow Web Server → App/API Server : TCP محدد فقط
8. Allow App/API Server → DB Server : TCP منفذ قاعدة البيانات فقط
9. Allow VPN Server → Internal Resources : حسب صلاحيات المستخدمين
10. Deny DMZ → Internal LAN : Any Other Traffic

من Internal LAN إلى DMZ

11. Allow Admin PC → DMZ Servers : SSH / RDP / HTTPS للإدارة فقط
12. Deny Any Other Unnecessary Traffic

- **كيفية حماية قاعدة البيانات الداخلية**

إذا كان الموقع يحتاج الوصول إلى قاعدة البيانات، فالأفضل أمنيا:

الحل الأفضل

عدم جعل Web Server يتصل مباشرة بقاعدة البيانات إن أمكن، بل عبر:

- Application Server داخلي
- أو Backend API داخلي

فيكون المسار:

```
Internet User → Web Server in DMZ → Internal App/API Server → Database Serv
```

المزايا

- قاعدة البيانات لا تكون مكشوفة مباشرة حتى لـ DMZ
- تقليل أثر اختراق Web Server
- إمكانية تطبيق تحقق وصلاحيات وتسجيل أفضل

إجراءات حماية إضافية

- استخدام حساب قاعدة بيانات محدود الصلاحيات
- تشفير الاتصال بين التطبيق وقاعدة البيانات
- منع أي اتصال من أي خادم آخر غير مصرح به
- تفعيل Logs و IDS/IPS .
- مراقبة محاولات الوصول غير الطبيعية

- **التحليل الأمني**

1. مبدأ أقل صلاحية:

كل خادم أو مستخدم يحصل فقط على أقل صلاحيات يحتاجها للعمل

مثال:

- Web Server لا يملك صلاحية كاملة على قاعدة البيانات
- VPN Users لا يصلون لكل الشبكة، فقط للموارد المسموح بها

2. التسجيل والمراقبة

يجب تفعيل

- Firewall Logs
- Server Logs
- IDS/IPS
- مراقبة محاولات الفشل في تسجيل الدخول
- تنبيهات عند السلوك غير الطبيعي

3. الحد من الحركة الجانبية:

في حال اختراق خادم في DMZ :

- لا يستطيع المهاجم الوصول مباشرة إلى Internal LAN
- توجد قواعد صارمة ومحددة

- يمكن كذلك فصل خوادم DMZ عن بعضها إن لزم

- **المقارنة بين Single Firewall DMZ و Dual Firewall DMZ :**

1. Single Firewall DMZ

يستخدم جدار ناري واحد بثلاث واجهات:

- واجهة للإنترنت
- واجهة لل DMZ
- واجهة للشبكة الداخلية

<u>المزايا</u>

- أقل تكلفة
- أسهل في الإدارة
- مناسب للمؤسسات الصغيرة

<u>العيوب</u>

- نقطة فشل واحدة
- إذا تم اختراق الجدار الناري قد تتأثر كل المناطق
- عزل أمني أقل من التصميم الثنائي

2. Dual Firewall DMZ

يستخدم جدارين ناريين :

- الأول بين الإنترنت و DMZ
- الثاني بين DMZ والشبكة الداخلية

<u>المزايا</u>

- أمان أعلى
- عزل أقوى
- حماية إضافية إذا فشل أحد الجدارين
- مناسب للمؤسسات التي لديها بيانات حساسة

<u>العيوب</u>

- تكلفة أعلى
- إعداد وإدارة أعقد

- يحتاج خبرة أكبر

- **التصميم الأنسب للمؤسسة**

الأنسب : Dual Firewall DMZ

<u>السبب</u>

لأن المؤسسة الجامعية تحتوي على:

- بيانات طلاب وموظفين
- أنظمة إدارية حساسة
- خدمات عامة متاحة للإنترنت

وهذا يتطلب مستوى حماية أعلى.

استخدام Dual Firewall يعطي عزلًا أفضل بين الإنترنت والخدمات العامة والشبكة الداخلية، ويقلل احتمال انتقال الهجوم إلى الأنظمة الحساسة.

- **الخلاصة النهائية**

التصميم الصحيح هو:

- وضع الخوادم العامة داخل DMZ
- إبقاء قواعد البيانات والأنظمة الحساسة داخل Internal LAN
- منع الوصول المباشر من الإنترنت إلى الشبكة الداخلية
- السماح فقط بحركة مرور محددة جدا بين DMZ و Internal LAN
- استخدام Duall firewall لأنه الأنسب للمؤسسة ذات البيانات الحساسة