بسم الله الرحمن الرحيم

جامعة الملك سعود
كلية علوم الحاسب و المعلومات
قسم نظم المعلومات

المنطقة المنزوعة السلاح
(المنطقة المحايدة)
Demilitarized Zone (DMZ)

إعداد : م. سليمان بن هيشة

إشراف: د. خالد الغثبر

مقدمة

أطلق مصطلح المنطقة المنزوعة السلاح على المنطقة الجغرافية المحايدة بين الأطراف المتنازعة، وصار هذا المصطلح يستخدم في شبكات الحاسب للدلالة على المنطقة الشبكية الفاصلة والمحايدة بين شبكة المنظمة الخاصة والشبكة العالمية كوسيلة لحماية شبكة المنظمة. [4]

شكل 1: *المنطقة المنزوعة السلاح بين الكوريتين الشمالية والجنوبية – الشريط الأبيض الفاصل -*

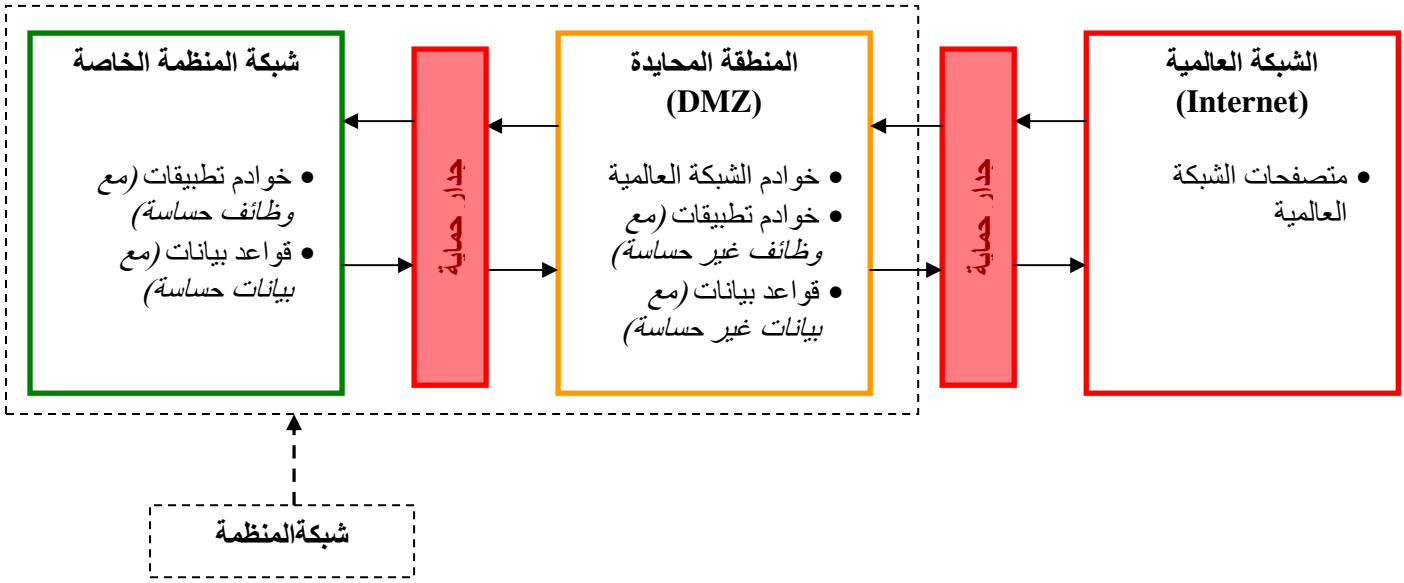
تعريف

يعتبر التصميم المادي للشبكة (Network Topology) من العوامل الأساسية لأمن الشبكات، وحتى لو تم تعديل هذا التصميم لأسباب أمنية، فإنها في النهاية لابد أن تعكس متطلبات المنظمة ومتطلبات مستخدميها، ومن هنا أتت فكرة مناطق الشبكة (Network Zones). [1]

المنطقة المنزوعة السلاح هي واحدة من هذه المناطق الشبكية والتي تستخدم لتقليل الأخطار المحتملة على شبكة المنظمة الخاصة من الاتصالات الغير المصرحة القادمة من الشبكة العالمية وبالتالي امكانية تسرب بيانات المنظمة السريّة.

في هذه المقالة سنشير إلى المنطقة المنزوعةالسلاح ***بالمنطقة المحايدة***.

المنطقة المحايدة

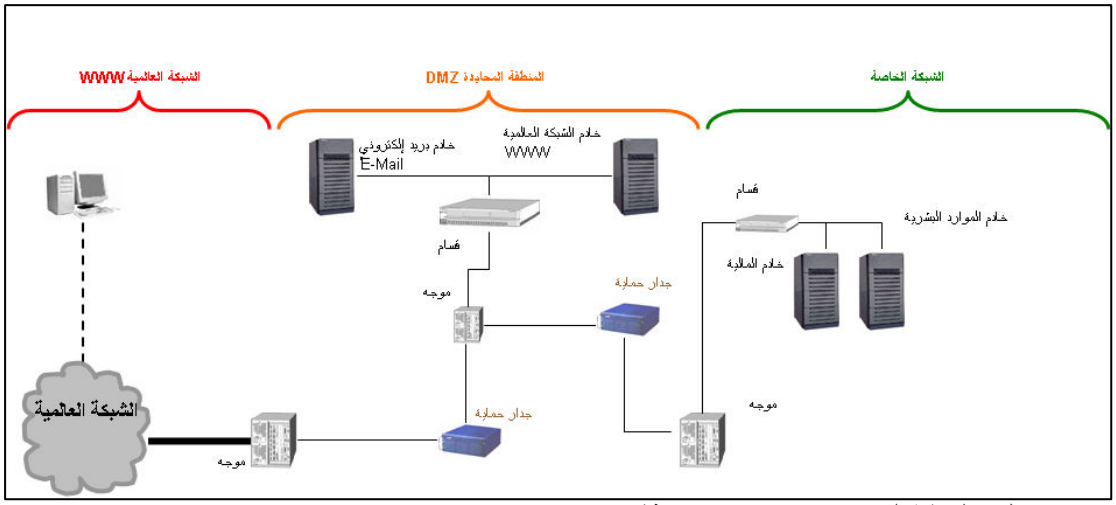


شكل 2: *المنطقة المحايدة (تصميم منطقي)*

كما نرى في الشكل 2 أن بإمكان مستخدمي الشبكة العالمية من الاتصال بالمنطقة المحايدة من شبكة المنظمة لكن ليس بإمكانهم الدخول إلى شبكة المنظمة الخاصة.

في الشكل 2 أيضا نرى جداريين ناريين، الهدف من الجدار الناري الأول بين الشبكة العالمية والمنطقة المحايدة من شبكة المنظمة هو حماية الخوادم الموجودة في المنطقة المحايدة - والتي بطبيعتها لابد أن تكون مرئية للعالم - من الهجمات عن طريق الشبكة العالمية، وهذه الحماية بناءا على الفلترة كالسماح لبروتوكلات معينة بالمرور مثل (HTTP, HTTPS) ومنع البرتوكولات الأخرى مثل (FTP, Telnet). [1]

والهدف من الجدار الناري الثاني بين المنطقة المحايدة والمنطقة الخاصة من شبكة المنظمة هو تزويد حاجز أمني مقوى لحماية المنطقة الخاصة، وأيضا كما في الجدار الثاني هذه الحماية بناءا على الفلترة كالسماح لبروتوكولات معينة بالمرور مثل (ODBC, JDBC) و يجب أن تكون الفلترة في هذا الجدار الناري مقيدة أكثر من الجدار الناري الأول، ففي حالة اختراق الجدار الناري الاول فإن احتمالية اختراق الجدار الناري الثاني أقل. [5]



شكل 3: *المنطقة المحايدة (تصميم فيزيائي - **مثال**)*

الخوادم التي يجب وضعها في المنطقة المحايدة

بشكل عام أفضل مكان للخوادم وقواعد البيانات المعدة للتعامل مع الشبكة العالمية هو منطقة الشبكة المحايدة، ومن الأمثلة على هذه الخوادم التالي: [4][1]

- خوادم الشبكة العالمية (Web Servers)
- خوادم بروتوكول نقل الملفات (FTP Servers)
- خوادم الاتصال البعيد
- خوادم البريد الإلكتروني

اجراءات خاصة للمنطقة المحايدة [2] [1]

- تقوية الخوادم من خلال فحص و تقليص الثغرات الأمنية. وذلك لأن المنطقة المحايدة عرضة للاختراقات القادمة من الشبكة العالمية.
- تعطيل الخدمات الغير مستخدمة، مثل الحسابات الزائدة و خدمة نقل الملفات (FTP).
- عمل فحص و تدقيق دوري لأنشطة الخوادم.
- التأكد من تركيب آخر التحديثات للخوادم.
- التأكد من أن الخوادم مجهزة بالشكل الكافي و المطلوب.

تحديات المنطقة المحايدة

- ***الأداء***:بطء أداء الشبكة بسبب الزيادة في عدد الأجهزة والموجهات[2] ، وهذا لأن المنطقة المحايدة تعتبر تقنيا كشبكة فرعية ، وانشاء شبكة فرعية يختلف عن التوسع في الشبكة نفسها.
- ***الإدارة***:ارتفاع تكلفة إدارة ومراقبة وصيانة الشبكة[2]، و هذا ناتج عن إضافة شبكة فرعية.
- ***المرونة***: قد لاتتوافق جميع التطبيقات مع هذه المعمارية[2]، فإضافة شبكة فرعية قد يتعارض مع معمارية شبكية تحد من الشبكات الفرعية.

تقنية أوعية العسل (Honeypots)

هي تقنية تستخدم في المناطق المحايدة لابعاد الاختراقات المحتملة على شبكة المنظمة، و هي عبارة عن خوادم مزودة ببرامج و بيانات تظهر و كأنها موثوقة و صحيحة لتوجيه انظار المخترقين إليها و صرفهم عن الخوادم الحقيقية.[1]

فائدة أخرى من هذه التقنية ألا وهي اعطاء انطباع عن أساليب المخترقين للاستفادة منها في صد هجماتهم وتطوير أنظمة الحماية. لكن عدم تجهيز هذه التقنية بالشكل الصحيح قد يشكل خطرا على شبكة المنظمة!، لأن هذه الخوادم تحاول محاكاة الخدمات المقدمة من الشبكة، وبدلا من أن تكون محاكاة قد تكون تنفيذ فعلي للخدمة. [1]

خاتمة

كما رأينا في هذه المقالة فإنه إذا كان لابد من اتصال بين شبكة المنظمة والشبكة العالمية فأفضل طريقة هي إستخدام المنطقة المحايدة[3]، وبهذه الطريقة نحمي الشبكة الخاصة للمنظمة من الاختراقات المحتملة عن طريق الشبكة العالمية.

المراجع

[1] M. Ciampa, "Security+ Guide to Networking Security Fundamentals", Second Edition, Thomson Course Technology, 2004.

[2] K. Tracy, "E-Business Security – An Overview", North Central College, Lucent Tech., http://csc.noctrl.edu/f/kwt/netsec.ppt. (April 25, 2005)

[3] SANS, "DMS Lab Security Policy", DMZ_Lab_Security_Policy.pdf, http://www.sans.org/resources/policies/DMZ_Lab_Security_Policy.pdf. (April 25, 2005)

[4] Defense Information Systems Agency, "Realizing the Net-Centric Vision", http://www.westhem.disa.mil/CD3/WWW_html/briefings/DMZ_22April04.ppt. (March 30, 2005)

[5] M. Kerr, "Case Study - Windows 2000 ISA Proxy Server Authentication Inside a DMZ.", SANS, http://www.sans.org/rr/whitepapers/casestudies/861.php. (April 22, 2005)