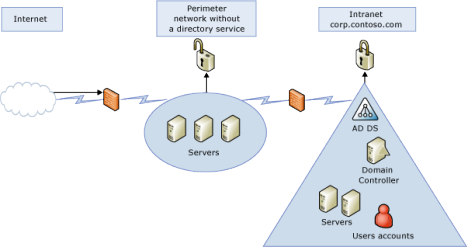
In this new series of articles, I am writing about some stressful kind of **Active Directory deployment** which is the **deployment within the perimeter network or the DMZ**. Many people believe that deploying Active Directory in the perimeter network is not the right decision because of the security risks imposed on the organization’s directory service. In this article in the series, I am going to discuss different deployment models of AD in the perimeter network.

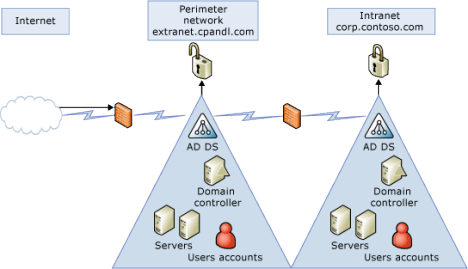
But before we start, there might be this question of **why** we need to deploy AD in the perimeter network in the first place and that’s simply because of the type of services being offered in that part of  the network to the outside users. There could be services like **Sharepoint Server, SQL Server, Office Communication Server or even a VPN Server** functioning in the perimeter network and all of them require access to the directory service of the network. So in any ways they require access to it and there should be a way of deploying that in the DMZ. this is WHY… So, below is an illustrated and descriptive list of different designs or models:

**1- No Active Directory Domain Services**

[](http://esihere.files.wordpress.com/2011/04/1.png)

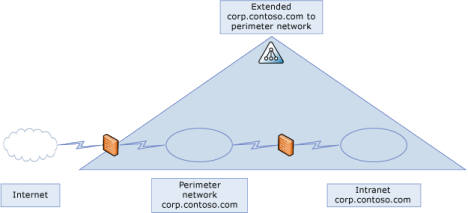
This simply means that we **do not create any connectivity between the directory service** in the network and **any of the other services**. You may prefer **using the servers’ own SAM (Security Accounts Manager) database file** which stores the local user and group accounts but that is **tough**, isn’t it? Having to create all those user accounts in all those servers and even making a change once in a while is another trouble. Besides, there are a lot of other **disadvantages** such a design could bring about like the**lack of security, the lack of a central management** and so more.

**2- Isolated Forest Model**

[](http://esihere.files.wordpress.com/2011/04/2.png)

As it is shown in the picture, it is possible by **creating two different forests** for the intranet and the perimeter networks. In this way we have the directory service in the perimeter network but still the**perimeter network is isolated from the rest of the network** meaning that any update on the directory services inside the intranet (Like adding or modifying user accounts) **will not affect the directory services in the perimeter network** and vice versa. And the **disadvantage** with this design is the type of Domain Controller that you are going to put in the perimeter network in this design is going to be a writable one, so there is this **risk** that if the**Domain Controller gets hacked**, then the data on the Domain Controller could be in danger of modification and this change will be replicated to all the other Domain Controllers in the perimeter network. **Another disadvantage** is that there is**no connectivity between the forests**and if the domain users in the intranet require access to any of the resources in the perimeter network, **it is not possible** to give them such an access since there is no connectivity between the forests.

**3- Extended Forest**

[](http://esihere.files.wordpress.com/2011/04/3.png)

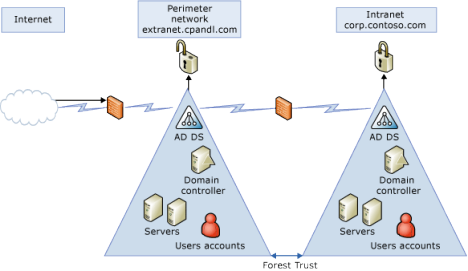
In this model we have **one single forest covering both the intranet network and the perimeter network**. This could be a good or bad design depending on your choice.

The**bad choice** is when you put **a writable Domain Controller in the perimeter network** and since the data on the Domain Controllers **gets replicated** between the intranet and the perimeter network, any changes by a hacker on the DC in the perimeter network could be replicated to all the DCs inside the intranet.

The **good choice** is using a **RODC (Read-Only Domain Controller) inside the perimeter network** which is in replication with the DCs inside the intranet but are by nature**Readable only** or as we call them **Read-Only Domain Controllers.** This way if by any chance one of the DCs in the DMZ is at risk of getting penetrated,**their data is not at risk of getting changed.**

Later on we will talk more about the RODCs in this series.

**4- Forest Trust Model**

[](http://esihere.files.wordpress.com/2011/04/4.png)

This is **one of the best designs** where there is a separate forest for both the perimeter and the intranet networks just like the Isolated Forest Model but**there is a trust between the two forests.**

The trust could be **unidirectional** meaning that we can only**let the intranet users access the resources inside the perimeter network**. For example, if you have a **SQL server in your perimeter network** and you want both your intranet users and outside users to access that server, then you could follow this model to have two forests and make a unidirectional trust between them making the server in the DMZ accessible to the intranet users but still preventing the outside users in the perimeter network to access any of the resources inside the intranet.

A **drawback** to this model is the cost of administration of two different forests.