



Article published on November 30th 2011 | [Internet](#)

With the consumerization in IT nowadays; the various mobilization and connectivity of devices as well as the explosion of a number of Web based applications, it has driven many of us to use the Internet and related technologies in ways different than before. These innovative trends in technologies have made businesses grow more competitive and increase their productivity so that they could also create new opportunities for the global market. This has also dramatically changed how business networks work nowadays; companies have pushed well beyond their old boundaries all with regard to the output and the speed. Unfortunately, the security infrastructure of networks, security methods like penetration testing and security tools haven't evolved together with the changing business networks.

Most of the time security administrators are forced to make a trade between the things they can and cannot accomplish, especially when it regards to the control and monitoring of new company network services. With the little visibility they have and the input of new services that are delivered to the systems it could led to possible negative effects to the system. Fortunately, there is a solution that can provide better foundation needed to protect the dynamic changes in the network structure and the services they have and it is network segmentation.

Network segmentation is complex procedure, but its basics are pretty straightforward. We could say that it is a process of logically putting network assets, applications and resources in groups. When it comes to introducing network segmentation into the system there are 4 key factors that have to be taken into consideration first.

Gaining Visibility

The first thing to consider is gaining visibility in the network. If the network administrators do not understand or recognize the traffic profiles on a proposed segment when it comes to inbound or outbound communication, then the access controls that have been implemented will all end as failures. It is important to understand how the segmented network is exactly used. Administrators will find themselves finding a connection on what they believe is occurring and what is indeed occurring on the system.

Protect Inbound or Outbound Communication and Resource Requests

Security has been always the primary goal of security administrators. If they do not have the knowledge, skill, tools, training like penetration testing training or other security training and the ability to protect the resources of a segment, then that goal won't be met. Simple controls aren't enough, administrators must have the ability to detect any possible threat and do instant action against it.

Implementing Granular Controls on the Traffic, the Users and the Assets

All of the data that will be going in and out of the segment must be controlled. If the security administrators have implemented protection, then the next thing to implement is the communication policy of the organization. Even if there is an understanding regarding the communication taking place with a certain segment and from a source coming from the outside, there should be controls that have to be implemented. It is a 2 step process, first is detective controls and the second is the

preventive controls. This way the administrator can identify and investigate unexpected traffic and prevent them if they are found to be malicious.

Denying Inter-Segment Communications

When there is visibility, protected communications and implementation of access policy, the last thing to do is denying all inter-segment traffic. When the policy is implemented, the segment will be separated from the network and that unit will be able to operate on its own.

Any approach towards network segmentations must follow the four steps; however, administrators must focus on one segment at a time for better results. They should begin with areas, which are easily segmented. At the start, implementing the four steps in the few segments will be difficult, but in the long run, the rewards of limiting the areas of risks and compromise by segmenting each areas and putting controls on them will be worth the trouble. In fact, if the security administrators will perform security audits or pen test, the segmented areas easily addressed.

The changing technological innovations continue to drive businesses forward “ pushing the scale, scope and performances of their networks. Companies has to be ready at all times, having a security approach that provides visibility, understanding as well as controls in order to protect their dynamic networks.

Article Source:

<http://www.articleside.com/internet-articles/protecting-business-networks-by-using-network-segmentation.htm> - [Article Side](#)

[Eccuni](#) - About Author:

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in cybersecurity and e-commerce. It is the owner and developer of 20 security certifications. EC-Council has trained over 90,000 security professionals and certified more than 40,000 members. These certifications are recognized worldwide and have received endorsements from various government agencies. They also offer trainings in penetration testing.

More information about EC-Council is available at www.eccouncil.org, a [pen test](#), a [penetration testing](#), a [penetration testing training](#)

Article Keywords:

Network Segmentation, pen test, penetration testing, penetration testing training, Business Networks, consumerization, global market, Outbound Communication, Security, security training, Granular, Controls, communication policy, dynamic networks, E-Commer