Next Generation Enterprise Networks

Date	03/04/2012
Version	1.2
Author	Anton Hofland

Abstract

Securing enterprise networks has been a challenge for the IT industry for many years. Today, in addition to threats from outside, security and privacy professionals consider the insider threat as the number one problem. Technology developments and the rapid adoption of consumer technology in enterprise environments, often driven by employees and third parties, are feared to further weaken enterprise network security.

This paper proposes a new design principle for enterprise networks, based on a fundamental rethink of the assumptions underlying enterprise network design. By designing, implementing and operating an enterprise network using the 'Protected Core' design principle, enterprises can surmount the challenges created by today's technology developments without putting user experience and productivity at risk.

Next Generation Enterprise Networks

In the last few years new challenges to enterprise network security have arisen as a result of the very rapid technology development and technology adoption. Directly or indirectly enterprise network security has been a topic of many publications. The three publications below are a very recent selection from a flurry of papers referring to a never-ending stream of security challenges and breaches. These papers clearly make the case that enterprises need to take action urgently to meet the security challenges head on:

1. A report by Trustwave, which suggests that anti-malware software is unable to prevent data breach attacks on the enterprise.

2. A presentation showing the results of a recent opinion poll, performed by Ziff-Davis, on the sentiments within enterprises with respect to the security threats caused by the mobile technology revolution.

3. An article in the New York Times, which describes the pre-cautions taken by many government agencies and some commercial organisations with respect to device security for staff traveling to China or Russia.

Of course, what action is taken depends entirely on what is determined to be the root cause which enables the ever increasing number of security challenges and breaches. In 2024Sight's view the root cause of most security challenges and breaches is the design principle used for enterprise networks. This paper will make the case that by using a different design principle, enterprise networks can be designed, implemented and operated so that they deal elegantly with the security challenges and prevent security breaches.

The Traditional Enterprise Network

Today's enterprise networks are designed using the so-called 'Hard Shell - Soft Core' design principle. This design principle is based on the assumption that threats to an enterprise network stem solely from the outside. Accordingly, the enterprise network can be secured by installing malware scanners, firewalls and security devices on the perimeter of the network (Hard Shell). In line with this design principle, it is not necessary to protect the inner parts of the enterprise network, thus leaving the application and the data open and accessible to those within the enterprise (Soft Core). A strong password policy and an internal anti-malware solution are considered to be sufficient to protect the network, the applications and the data.

Figure 1 shows the typical layers of an enterprise network design based on the 'Hard Shell – Soft Core' design principle. An inner layer of firewalls separates the enterprise network from

the so-called DMZ (the De-Militarised Zone), in which the externally facing servers, including internet facing servers, are located. The DMZ is separated from the internet by an outer layer of firewalls to maximise protection.

Recent research and surveys suggest that as much as 21% of attacks on enterprises come from within (Cyber Security Watch Service 2011) and that 58% stem from outside with a further 21% stemming from unknown sources. According to the report, internal attacks have typically been more damaging. However, in 2024Sight's view it is increasingly futile to even distinguish between internal and external attacks, as many breaches of security seem to have come about as a result of a combination of circumstances, both internal and external to the enterprise.

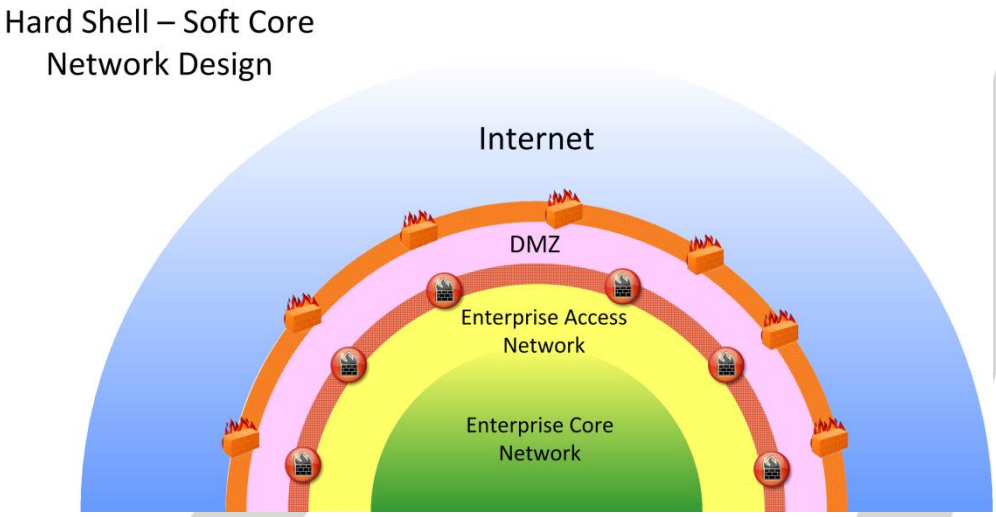

Figure 1

The following example illustrates this point. A recent breach of security at a security devices manufacturer was brought about by malware that was sent as an e-mail attachment. Apparently, the malware created a back door on an internal device, allowing the external perpetrators to get hold of extremely sensitive, security related information. It will take time before the full impact and damage of this particular breach and its wider implications are known.

As if the above is not sufficient ground to re-think the design principles of a network, there are change drivers at work, which will put the enterprise and its network even more at risk than they are today.

Drivers for Change

The environment, in which the enterprise network operates, has morphed significantly in recent years. Today's enterprise network has to be able to deal with the challenge of:

1. Staff bringing their own devices (known as BYOD or 'Bring Your Own Device'): With the advent of cool consumer technology enterprise IT managers are increasingly required to accommodate employees bringing their privately owned consumer devices and connecting them to the enterprise network. Instead of using enterprise provided devices to perform their jobs, the employees want to use their personally owned devices to access company applications and data, while at the same time using the devices for personal activities.

There are many issues with BYOD such as malware management, installation and maintenance of enterprise applications on an ever increasing variety of platforms, and, most importantly, the secure storage of enterprise data on BYOD devices. While the issue of storing data on end-user computing devices is not new, it is made worse by the BYOD trend. By default, these devices do not provide the enterprise with any means to manage, encrypt, delete and restore data. With an enterprise owned device the enterprise was able at least to install tools that would assist with this management issue. Some of these tools are also available for BYOD devices, but despite that, managing data on BYOD devices increasingly looks like a losing battle.

In addition, there is an increased risk with BYOD devices that personal data will leak into the enterprise network. Again, this issue is not new, but also made worse by the BYOD trend. Private and personal data being present on enterprise systems has been known to get enterprises into serious trouble. Music tracks, ripped DVDs and data from previous employers are the typical examples.

2. Third Parties, including visitors, consultants and contractors: Every enterprise will have visitors and many enterprises will use consultants and contractors for certain activities. In this day and age of smartphones, tablets and ultra-books every third party will be bringing along his or her own technology, expecting to have access to the internet for business or personal reasons. In addition, some third parties may need to access the enterprise's data and applications. Obviously, there is a challenge of how to provide the required levels of access to third parties without putting the security of the enterprise network, its applications and data at risk.

3. E-discovery: In the recent years there have been a significant number of cases where e-discovered information has been used in legal proceedings. E-discovery is the process of careful analysis of any confiscated data carrier, which, in the opinion of the authorities, may hold some form of information essential to legal proceedings. A data carrier in this context could be a tape, CD, DVD or a hard disk, but of course, it may also be a non-removable solid-state storage device of a tablet or mobile phone, i.e. the entire device.

   The e-discovery challenge has been around for a number of years, but with the advent of tablets and smartphones, coupled with the BYOD trend, it will become an ever larger challenge for enterprises. An enterprise needs to know at all times where all its data is and how its data can be recovered. As important, the enterprise also needs to know with near absolute certainty where its data is not. I.e. it should know it is not on mobile devices, tablets, private laptops, third party laptops and any other devices that are not directly under the control of the enterprise.

By introducing technologies such as Network Access Control and Mobile Device Management it is possible to cure many of the ills caused by the above change drivers. However, prevention is better than cure. I.e. by changing the underlying design principle for enterprise networks it is possible to prevent the ills from arising in the first place. It is time to abandon the 'Hard Shell – Soft Core' enterprise network design principle and to replace it with something more appropriate.

The 'Protected Core' Network Design Principle

In 2024Sight's view the only way to really overcome today's security challenges facing enterprise networks is by:

1. Accepting that in reality there are two distinctly separate enterprise networks, i.e. the Enterprise Core Network and the Enterprise Access Network. The Enterprise Core Network is the network, which connects to the enterprise server infrastructure and

which holds the enterprise applications and data. The Enterprise Access Network is the network to which employees and third parties connect.

2. Accepting that the Enterprise Access Network is as hostile a network as the internet itself.

3. Accepting that all who connect to the Enterprise Access Network need to be viewed the same way, and that in terms of risk there is no difference between an employee and a third party.

Based on the above it is possible to derive a design principle, which we shall refer to as the 'Protected Core' design principle.

The 'Protected Core' design principle is based on the idea that the Enterprise Core Network is the network to secure and internally harden. This can be achieved through various means such as very strict control on the use of elevated rights (i.e. administrator rights), encryption, internal firewalls and network segregation, intrusion detection and prevention, and strong password policies. Last but not least, the data flows into and out of this network are to be restricted and should be fully logged.

The design principle recognises that the Enterprise Access Network is in fact just that, i.e. an untrusted network, no different from the internet, which is used to view enterprise data and remotely control enterprise applications, but is NOT used to transfer data or applications to any connected device.

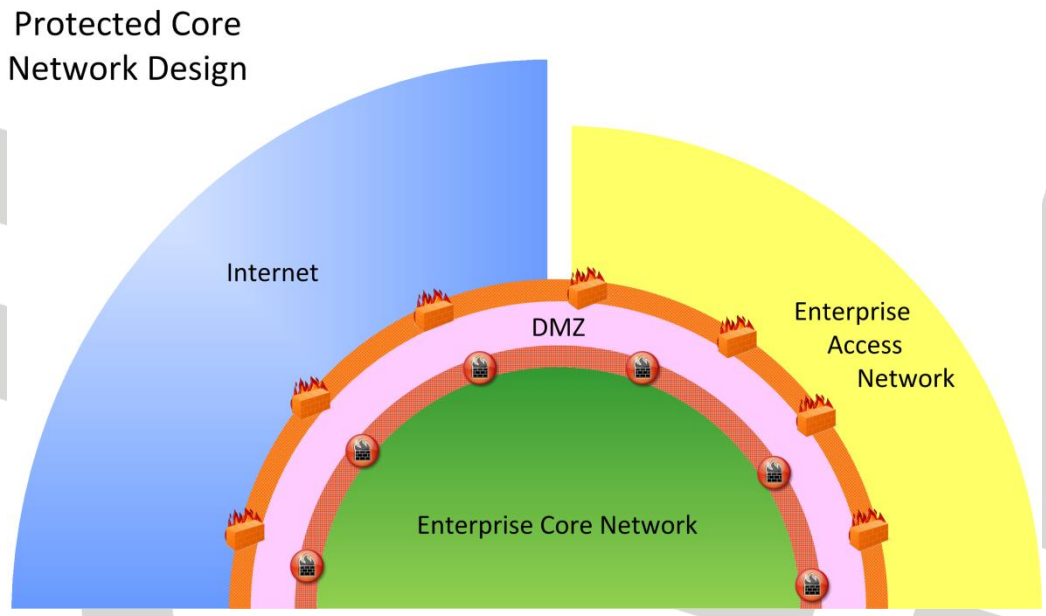

Figure 2

Figure 2 shows the layers of an enterprise network, which is designed using the 'Protected Core' principle. The Enterprise Core Network is directly protected by a layer of inner firewalls and a DMZ. The Enterprise Access Network is connected to the DMZ via a layer of outer firewalls. Devices connected to the Enterprise Access Network may only cross the layers of firewalls and DMZ to access the Enterprise Core Network by:

1. Using a fully encrypted, secured and logged Virtual Desktop Infrastructure (VDI). Even when using the VDI, the only servers in the core that are accessible from the Enterprise Access Network are the VDI servers. Further, the VDI should prevent drive mappings between connected devices and servers in the core. The VDI should also

block copy-and-paste style operations between applications running on the VDI in the core and applications running on any device connected to the Enterprise Access Network;

or

2. Establishing from an enterprise controlled and maintained device a secure connection using Virtual Private Networking (VPN) technology. All traffic going over this type of connection should be logged at the very least so that the enterprise can establish at a later date what data may be stored on the device.

Obviously, the second option is less strict and immediately reduces the level of security and the level of control that the enterprise has over its data. It should only be used if absolutely necessary.

Internet facing servers and any other externally facing servers, including any servers that face the Enterprise Access Network, are located in the DMZ and separated from the internet and the Enterprise Access Network by a layer of outer firewalls. Any traffic coming into the enterprise via the internet, via for instance e-mail and web, as well as traffic leaving the enterprise should be logged at the very least, if not strictly controlled.

Any device connected to the Enterprise Access Network and requiring access to the internet can optionally be provided with access by allowing a path from the Enterprise Access Network, through the DMZ out to the internet, while concurrent access via VPN to the core and directly to the internet is blocked. Observe that in this design the untrusted Enterprise Access Network is shielded from the internet by two layers of firewalls and a DMZ.

There is significant amount of technical detail to be specified should an enterprise decide to implement a 'Protected Core' network. With the advent of the various virtualisation technologies an enterprise network can be transformed to a 'Protected Core' design without significant impact on the user experience.

Reviewing the 'Protected Core' Design

The change drivers are reviewed below in the light of the 'Protected Core' design principle:

1. BYOD: An enterprise network designed using the 'Protected Core' design principle will deal inherently with the insecurities of BYOD devices. Enterprise applications are remotely controlled from the BYOD device and data can be viewed on the BYOD device, but no data or application is ever transferred to the BYOD device. There is no issue with application installation on the BYOD device other than the client side of the VDI. The VDI technology can offer shortcuts to enterprise applications on the BYOD device in the form of an overlay, thereby providing the end-user with an excellent experience resembling the running of the application locally.

   Obviously, even when connected to a 'Protected Core'-style network, the BYOD device should still be protected by malware management tools, which is the responsibility of the device owner. However, the risk of enterprise data leakage and data loss has been very significantly reduced. With this style of network it is impossible for private and personal data to leak into the enterprise from a BYOD device.

2. Third Parties: Third parties can connect to the Enterprise Access Network without difficulties and, as with employees' BYODs, they can be given selective access to enterprise applications and data as necessary. However, by default the third party will only be able to connect from the Enterprise Access Network to the internet. Therefore, the third party forms no threat to the enterprise or its data and there is no

issue of how to connect a third party. In fact, employee and third party are treated exactly the same.

3. E-Discovery: Implementing a network and infrastructure based on the above principles allows enterprise IT to know exactly where all data is and where it is not, thereby protecting the enterprise as well as the individual device owners. At the very least extensive logging of data transfers into and out of the Enterprise Core Network is possible, while strict implementations only permit the VDI to communicate between the different parts of the enterprise network. As a consequence of implementing this design, the enterprise can always know where its data is and in strict implementations the data can only be on the servers in the Enterprise Core Network.

In conclusion, by designing and implementing an enterprise network using a 'Protected Core' design an enterprise can implement networks that can surmount the challenges put to it by today's technology developments without putting user experience and productivity at risk. The author designed and supervised implementation of an early 'Protected Core'-style network in the Riffa Views International School in Bahrain.

Please observe that as a consequence of implementing a network based on the 'Protected Core' design principle, there is no enterprise data stored on any device, including enterprise provided laptops, desktops, tablets and smartphones (strict implementation only). That means that accessing enterprise data requires connectivity. Whilst this could be viewed as a disadvantage, it should be noted that good quality WiFi access is becoming more and more ubiquitous, even in flight (please refer to the In-Stat In-Flight Broadband Report).

Enterprise Network Investment Protection

In an enterprise network infrastructure, designed using the 'Protected Core' principle, the amount of data which traverses between the Enterprise Core Network and the Enterprise Access Network is inherently minimized. This is a benefit entirely due to the use of a VDI as the amount of traffic generated by this type of infrastructure is very much smaller than the amount of traffic generated in a traditional style network where applications run on the connected device. Consequently, by adopting a 'Protected Core' design, the lifespan of an established Enterprise Access Network can be significantly extended. Newly built Enterprise Access Networks can be leaner than is customary today in terms of bandwidth, the installed technology, space, power and cooling.

A technology which is eminently suitable to implement secure, energy-efficient, cost-effective and lean enterprise networks is Passive Optical Networking (PON). Please refer to other 2024Sight publications about PON as an enterprise access network technology.

About 2024Sight

2024Sight is a Vienna-based consultancy that focusses on specifying solutions to IT and IT-related problems that at first glance do not seem to have any obvious or elegant solution. In the recent past 2024Sight has designed and managed the implementation of a PON-based, converged building and enterprise access network for Arcapita Bank B.S.C. and the Riffa Views International School. 2024Sight also specified a high-density data centre using several innovative techniques, such as oxygen reduction to prevent fire and rack-based cooling. Subsequently, it managed and supervised the data centre's construction, testing and commissioning. Further, 2024Sight managed the deployment of a long-haul telecommunications fibre network connecting the United Arab Emirates, Saudi Arabia and Bahrain.

About the Author

Anton Hofland has more than 20 years' experience in IT, IT infrastructure and enterprise networking, gained mostly in the financial industry. Before establishing 2024Sight he was the Head of IT for Arcapita Bank in Bahrain. Previously he has worked for several major financial institutions in the City of London. He has also worked in the area of telecommunications regulation and has experience in the telecommunications industry. Anton holds a M.Sc. in mathematics and computer science from Delft University, Netherlands.