Next Generation Enterprise Networks

Anton Hofland, MSc
CEO
2024Sight

Securing enterprise networks has been a challenge for the IT industry for many years. Today, in addition to threats from outside, the insider threat is considered the number one problem. Technology developments and the rapid adoption of consumer technology in enterprise environments are expected—and feared—to further weaken enterprise network security.

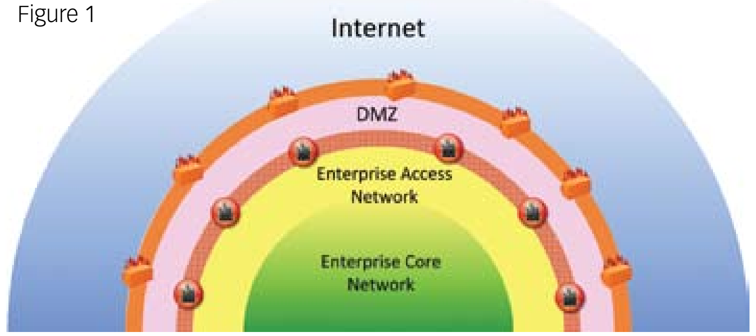
2024Sight proposes a new design principle for enterprise networks, based on a fundamental rethink of the assumptions underlying traditional design solutions. By designing, implementing and operating an enterprise network using the 'Protected Core' design principle, enterprises can surmount the challenges created by today's technology developments without putting user experience and productivity at risk.

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). Consequently, it is not necessary to also 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).

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. 2024Sight believes 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. In addition, we have identified change drivers at work, which will put the enterprise and its network even more at risk than they are today.

Hard Shell – Soft Core
Network Design

Figure 1



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 (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. 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. In addition, there is an increased risk with BYOD devices that personal data will leak into the enterprise network.

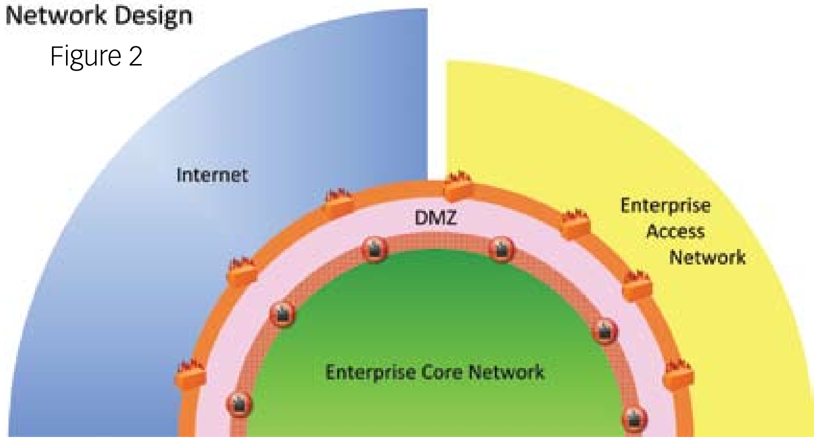
2. Third Parties, including visitors, consultants and contractors: In this day and age of smartphones, tablets and ultra-books, every third party will be bringing along his or her own technology, expecting to have access to the internet for business or personal reasons, in addition to needing access at times to the enterprise's data and applications.

3. E-discovery: In 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.

While technologies such as Network Access Control and Mobile Device Management are able to cure many of the ills caused by the above change drivers, 2024Sight thinks prevention is better than cure. It is time to abandon the 'Hard Shell—Soft Core' enterprise network design principle and to replace it with something more appropriate.

Protected Core
Network Design

Figure 2



The 'Protected Core' Network Design Principle

The only way to really overcome today's security challenges facing enterprise networks is by accepting that:

1. In reality there are two distinctly separate enterprise networks: the Enterprise Core Network, connecting to the enterprise server infrastructure and holding the enterprise applications and data; and the Enterprise Access Network to which employees and third parties connect.

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

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

The 'Protected Core' design principle takes this perspective into account and 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 'Protected Core' design principle recognizes that the Enterprise Access Network is in fact just an untrusted network, no different from the internet. It is used to view enterprise data and remotely control enterprise applications, but is *not* used to transfer data or applications to any connected device. Connection to the Enterprise Core Network is only possible by using a fully encrypted, secured and logged Virtual Desktop Infrastructure (VDI), or—by establishing from an enterprise controlled and maintained device—a secure connection using Virtual Private Networking (VPN) technology.

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

The 'Protected Core' design allows enterprises to implement networks that have security deeply embedded into them, enabling them to surmount the challenges presented to them by today's technology developments without putting user experience and productivity at risk. A 'Protected Core' network does not permit enterprise data to be stored on any device outside the core of the network, including enterprise provided laptops, desktops, tablets and smartphones (strict implementation only).

By adopting a 'Protected Core' design, the lifespan of an established Enterprise Access Network can be significantly extended, as the amount of data traversing between the Enterprise Core Network and the Enterprise Access Network is inherently minimized. 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). •

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.