Zeetta NETWORKS

NetOS powered by zeetta

WHITE PAPER

NETWORK SLICING – THE NEW WAY TO SECURE NETWORKS

With the number and variety of cyber-attacks increasing in today's connected world, your network is your first line of defence. Network architectures designed with 'defence in depth' principles in mind are better able to withstand a cyber-attack.

Traditional network design is inherently insecure

In 'traditional' network design, a flat or semi-flat network includes devices and end points that can communicate with each other directly, via a switch, without impedance. Such a network is very convenient and easy to administer, but offers little protection when the network is penetrated. Compromised devices are able to connect directly with all endpoints in such a network, which includes those that they ideally would not be able to see or communicate with, if the network were properly partitioned.

Recent cyber-attacks such as Wannacry, NotPetya and BadRabbit have affected a large number of endpoints in many organisations. These malware can use common techniques to discover and infect the other hosts, for example using vulnerabilities in Windows (e.g. WMI, SMBv1, PSExec). From there, they can infect other endpoints by using cached information in Windows tools or network scans.

These malware can infect all endpoints (servers, workstations, laptops) and can affect their data by, for example, encrypting their file systems and storage for ransom.

A massive cyber-attack could cost Fortune 100 companies upwards of £100m

Today's security technologies such as endpoint protection (Antivirus), network firewalls and Intrusion Prevention Systems (IPS) can block known patterns of malware. What they cannot do is detect day-zero malware, i.e. malware using penetration techniques that have not been seen previously, and so for which no identifiable pattern is known.

To further complicate matters, security experts are predicting that by 2020, 70% of these type of network attacks will be encrypted. Since encrypted traffic hides the payload, detection and prevention mechanisms based on known patterns will become less effective, and so the problem will become more complex.

Increasingly, existing security technologies will not be adequate to protect businesses. Current, pattern based, security technologies will not be sufficient to detect the malware and prevent its spread across the network. This affects IPS solutions within a network, and the virus detection software running on your laptop. So, new thinking is called for.

Most organisations have firewalls with thousands of rules. Many rules are outdated, unused and without documentation.

Because of performance limitations Intrusion Prevention Systems (IPS) are used either with minimum signatures, or process a small percentage of traffic.

Firewalls are an important element of a security architecture. As a complement to Deep Packet Inspection (DPI), firewalls create demarcation of traffic flows between hosts in networks. Many organisations can rely on numerous firewalls to secure their digital assets and workspaces. Firewalls have turned out to be operationally problematic as the rules upon which they are based become unmaintainable and so fail to evolve with the changing business.

Latterly, there has been an increasing emphasis on using Artificial Intelligence (AI) log analysis tools, which combine multiple data sources to detect anomalies and patterns of malicious behaviour within enterprise networks. These evolutions in security approaches are all indicative of the 'arms race' between cyber-criminals and the forces lined up against them.

Wannacry and Not-Petya were replicating themselves via standard SMB protocol to other endpoints.

Meanwhile, such protection is often insufficient. A malware can replicate itself amongst multiple hosts, and cause significant damage, before encountering a firewall. Moreover, malwares can be embedded within legitimate traffic between trusted hosts, and using trusted protocols, and so pass between networks through firewalls, and even be transparent to IPS systems.

These are real world, security concerns of CIOs today.

Network slicing – the simple way to isolate endpoints

Network slicing is an emerging concept both as a key element of 5G network architectures, and in other network domains. Network slices for endpoints and services can be used to logically isolate network traffic flows from specific hosts to specific parts of a network. Importantly, with NetOS, this can be done dynamically over heterogeneous network infrastructure.

In the enterprise domain, a network slice can be manifested as a SSID in a Wi-Fi network, as a VLAN in L2 networks, as IP sub-domains, or with other forms of encapsulation in other networks, such as access, LAN, WAN and DC. The logical slice, and the virtual network that it represents, is ***independent of the underlying physical network***.

Network Slicing is a modern SDN method to provision a virtual network between specific endpoints, servers and services over shared physical infrastructure.

The outcome is that the physical network resources are virtualised to provide multiple distinct 'sub-networks' over the same physical infrastructure, with strict isolation of traffic flows throughout the network.

The NetOS® Platform provides a secure solution

NetOS® is the world-leading network slice management platform from Zeetta Networks. NetOS® enables the dynamic creation and management of end-to-end network slices (or 'virtual networks') that can include multiple network types, aggregated into a single, manageable topology.

Creating network slices for your services helps isolate and secure them. Devices located in a network slice will be able to communicate only with specific other devices, based on predefined policies. For example, a network slice designed for your tills and relevant servers will only allow communication between tills to the server, and so can isolate those tills within a network that also, physically,

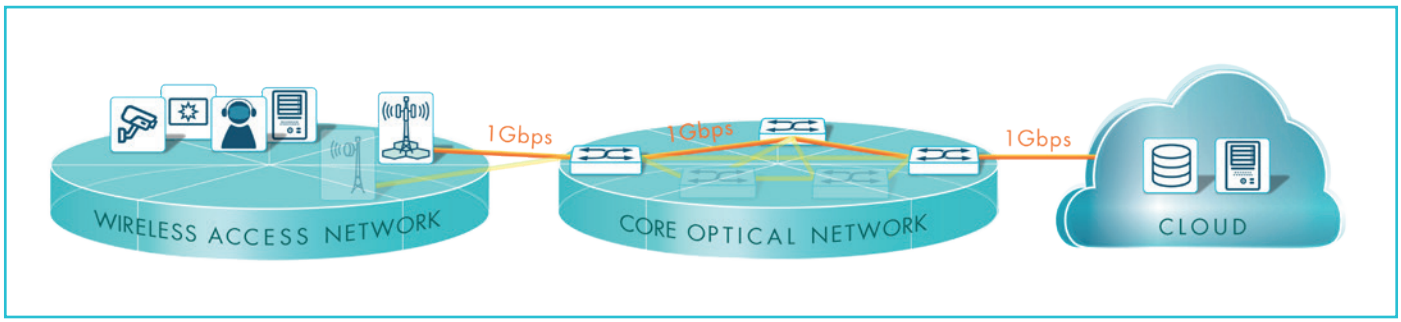

Fig 1. NetOS® can create on-demand 'network slices' with guaranteed Quality-of-Service and full control to support AR/VR Applications, CCTV video analytics, digital signage and more

Adding devices to the network

A key outcome of the ability of NetOS® to dynamically interact with your network is that it can automatically identify new hosts, and control which parts of the network they can access. This is especially important in multi-tenanted, multi-use environments, such as stadiums, malls and other public spaces.

serves the wider IT infrastructure for the organisation. Nothing in the tills will infect anyone else, nor will they infect the tills, and the money will keep rolling in.

NetOS® integrates with existing networking infrastructure as a network slicing controller to provision, manage and monitor network slices on your existing network. It helps you create a more secure IT infrastructure. With its open API environment it helps you do so dynamically, and on demand. Creating new services that add value to your IT environment is easy – including applications to identify and locate unwanted attempts to attack your network.

It is now much easier to allow for different users to connect to your IT infrastructure, knowing that they can be automatically and safely quarantined into user or service specific slices. Given the open APIs on NetOS®, you can develop your own business logic for how your network responds when devices are connected or moved.

Even better, with the ability of NetOS® to map your network infrastructure assets to maps and diagrams of your buildings and facilities, you can tell where devices are in your physical space when they are connected to the network. This allows you to both locate your own assets, and spot when something potentially untoward is happening.

Using NetOS® to create network slices helps reduce the risk of zero-day attacks on your network by giving you the programmable flexibility and adaptability you need to create partitioned network services. NetOS® helps your organisation limit the impact of cyber-attacks to minimum, and allows you to make more efficient and effective use of your network assets.