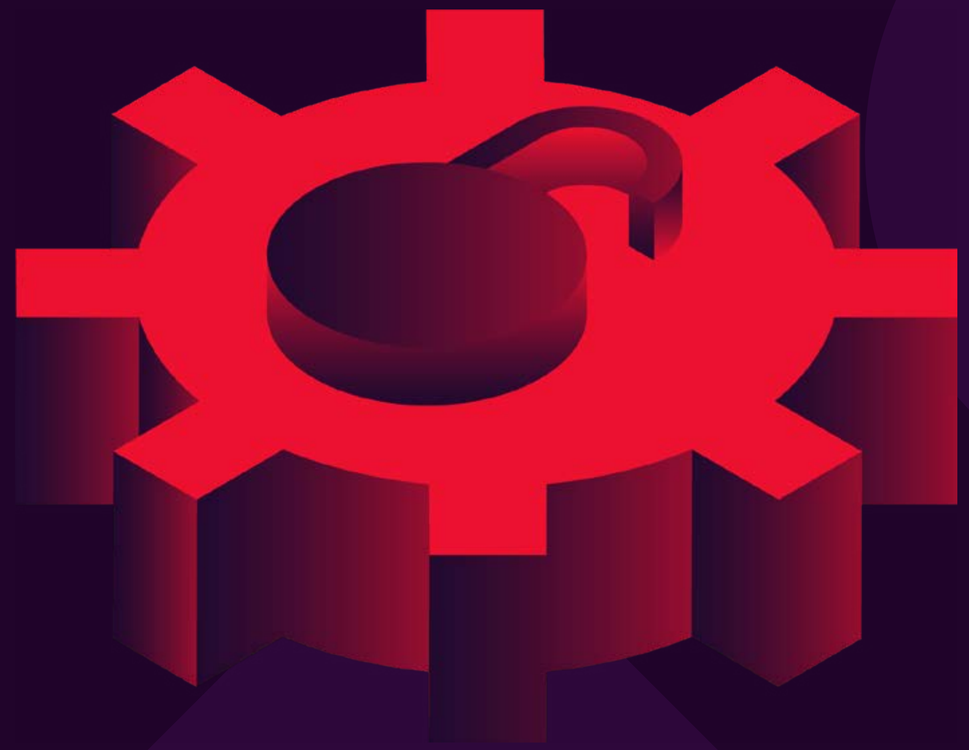
FourNet®

Quick Guide on

Protecting the Network Edge

Enter Guide



Copyright 2022®

Welcome to our Quick Guides to Cyber Security Series.

These five guides have been created to give you an overview of the key pillars and solutions needed to overcome the challenges arising from Cyber threats.

Other guides in our security series:

Secure Infrastructure | Quick Guide on Edge/Perimeter Security

Secure Infrastructure | Quick Guide to Endpoint Security

Secure Infrastructure | Quick Guide to Cloud Security

Secure Infrastructure | Quick Guide to Data and Compliance

Secure Infrastructure | Quick Guide to Socially Engineered

In these guides, we outline all the major risks and threats, security trends, common challenges, and impacts. Finally, we consider the best ways to calculate and mitigate the risks to your organisation, the key measures which should be introduced, and outline how FourNet's best-in-class security solutions can help.

If you take one concept from this series, it is that effective cyber security requires a layered approach to be successful. Also be mindful that compliance does not make an organisation secure and relying solely on technology to provide the solution won't combat the inherent risks posed by humans.

Building the right security culture and strategy is like Lego, needing many pieces to intersect and interplay to help mitigate the increasing level of risk our organisations face.

Copyright 2022®

Contents

01 Securing the network and edge

02 Protecting the edge What steps can you take?

03 Key areas of consideration for protecting the edge

04 How FourNet Can Help

Copyright 2022®

01 **Securing the network and edge**

02 Protecting the Edge What steps can you take?

03 Key Areas of consideration for protecting the edge

04 How FourNet Can Help

Securing the network and edge

The network's perimeter is the first line of defence for any organisation and a critical layer in deploying a robust cyber security solution.

The principles of perimeter security go back thousands of years. Walls, moats, sentries, and geese are historical ways to ensure the detection and defence of valuable assets held within a location.

Any security breach can harm your organisation by disclosing sensitive information or causing a loss of revenue. To avoid such damage, organisations must understand the challenges of perimeter security and implement proper solutions.

Historically we have seen a centralisation in computing, with local area networks in data centres allowing for robust security, hiding valuable data and assets behind layers of security defences.

However, In the digital world, technologies and interconnected systems have converged, meaning that the reliance on network security has never been greater, and the perimeter is no longer a fixed and visible horizon. This new way of delivering services without borders has created a new network edge.

Edge computing is often defined as computing that happens at the edge of a network. since the core of the network is the data centre or cloud, the broader corporate campus, branch offices and retail locations can be considered at the edge of the network.

Network security architectures that place the enterprise data centre at the centre of connectivity requirements are an inhibitor to the dynamic access requirements of digital business.

Gartner



Copyright 2022®

01 Securing the network and edge

02 Protecting the Edge What steps can you take?

03 Key Areas of consideration for protecting the edge

04 How FourNet Can Help

What the network edge includes:

Cloud Border Routers

The Border router is the demarcation point between the network and the Internet Service Provider (ISP). It is the point where connection and liability end for the ISP and the entry point to your network.

Forwarding routing information and packets of data, they provide rudimentary protection such as identifying traffic with invalid Internet Protocol addresses (IP).

Firewalls

Traditionally Firewalls have sat at the perimeter/ edge with predetermined configuration and rules, setting out what traffic is allowed to pass through it. This enforces security policies and limits the ingress and egress of data to defined IP addresses within the network.

Screened Subnets / De-militarised zones (DMZ)

DMZ and screened subnets refer to networks containing public services offered directly to and protected by a firewall or other filtering devices.

Network Intrusion Detection System (NIDS)

Using network traffic monitoring, NIDS uses pattern matching and algorithms to inspect and interrogate traffic to identify suspicious traffic, such as port scans or exploitation attacks.

“Research proved that 16 percent of web-server vulnerabilities have publicly available exploits. The availability of TCP network port 80 means that data can be exchanged via the HTTP protocol. And as we know, HTTP traffic is transmitted without encryption, meaning attackers can intercept it”.

Source (Threat Post)

Copyright 2022®

01 Securing the network and edge

02 Protecting the Edge What steps can you take?

03 Key Areas of consideration for protecting the edge

04 How FourNet Can Help

Common challenges in securing the network edge

Cybercrime is a growing threat, and a common form of attack used by cybercriminals against perimeter defences is remote access service attacks.

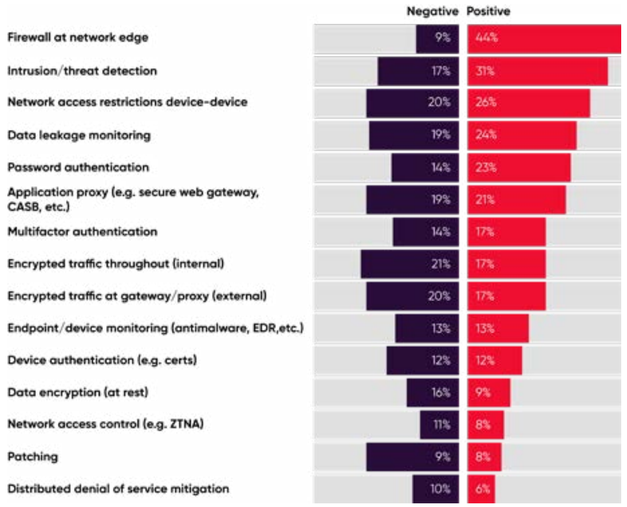
These types of attacks are particularly concerning because they can be used to penetrate your network and infect other devices. Many of the threats you will face tomorrow will come from today's vulnerabilities, and the first step in applying adequate security measures is to understand your current perimeter vulnerabilities.

Common challenges facing security teams with Perimeter security are

- Proliferation of misconfiguration in devices and applications
- Poor control of Privileged Access Management
- Inoperability within tools and systems
- Lack of visibility
- Outdated controls for evolving IT infrastructure

It is common knowledge that security teams face challenges with staff, skills and knowledge shortages, overlay this with increasingly complex infrastructure, and threats, and it is no surprise that some basic security protocols can sometimes be missed, leading to a failure in cyber defences.

In your opinion, which of the following would provide the most significant cost-benefit for your edge security and which would not be worth deploying? (% of respondents)



Global survey of 1520 security practitioners from organisations with 1,000+ employees (except US public sector and energy and utilities) conducted September 2021

Source: AT&T Cybersecurity- 2022 Securing the Edge

Copyright 2022®

01 Securing the network and edge

02 Protecting the Edge What steps can you take?

03 Key Areas of consideration for protecting the edge

04 How FourNet Can Help

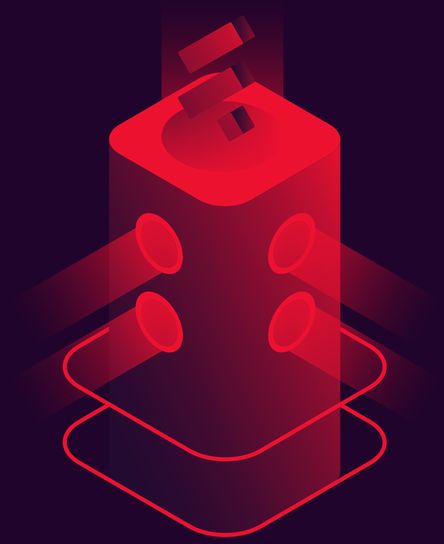
Protecting the Edge – What steps can you take?

There is no single solution or defence that can deliver complete protection of your perimeter, but steps can be taken to harden defences and provide situational awareness when threats arise. When reviewing your cyber security, it is worth keeping in mind the five D's, which are **Deter, Detect, Deny, Delay** and **Defend**. Many also like to add a sixth 'D' which is Demarcation.

Building a secure network perimeter needs to start with detecting and disabling active services that are not used and insecure protocols that may provide a gateway to the wider network. This will make it harder for malicious actors to gain access to key systems within your organisation.

6 Edge Computing Security Strategies

1. Use access control and surveillance to enhance the physical security at the edge.
2. Control edge configuration and operation from central IT operations.
3. Establish audit procedures to control data and application hosting changes at the edge.
4. Apply the highest level of network security possible between devices/users and edge facilities.
5. Treat the edge as a part of the public cloud portion of your IT operation.
6. Monitor and log all edge activity, particularly activity relatingto operations and configuration.



Copyright 2022®

01 Securing the network and edge

02 Protecting the Edge What steps can you take?

03 Key Areas of consideration for protecting the edge

04 How FourNet Can Help

Key areas of consideration for protecting the edge

Next-Generation Firewalls

Cyber threats advance, and so does the technology that repels them. Next-generation firewalls deliver enterprise security for the edge with advanced threat protection and full visibility. They allow organisations to not only protect the perimeter but ensure malware doesn't slip into the network via encrypted traffic routes. In addition, next-generation firewalls can detect and secure insecure protocols that may provide a gateway to the wider network.

Network Monitoring

Network monitoring is a critical part of any security operation. Being able to focus resources and time in the right places ensures that you can deliver an effective security strategy. Being able to quickly identify, interrogate and quarantine network activities in real-time, ensures you can react to the right things at the right time. With one of the key challenges being visibility of the network, having monitoring in place can remove the burden and stresses around managing a complex IT environment.

IOT and Mobile Security

The proliferation of devices connected to the network has created an additional challenge for security professionals. The number of potential entry points into the network has increased exponentially, and many of those devices, including mobile phones, have access to the network.

While having solutions in place to allow visibility of the network is important, ensuring that adequate measures are taken, such as Mobile Device Management (MDM) can give security professionals additional tools in the fight against cyber-attack.

Vulnerability Management

Knowing the network's strengths and weakness is a critical element in choosing where to invest budget and time. The best way to do this is to test the network in a controlled way to highlight potential vulnerabilities. This can be done with a perimeter scan which is performed outside of the host network and mimics the behaviours of potential attackers.

The idea behind this type of scanning is that an attacker will not want to expose themselves by trying to gain access directly into your system; instead, they will try to find an entry point from outside your network. A perimeter scan can help identify these weaknesses so that you can determine how best to protect them.

A Zero Trust Approach

Some instances of applying a zero-trust network access model (ZTNA) can be too prescriptive, but the need to ensure devices are authorised to access applications and the network is sound. A "never trust, always authenticate" approach to ensuring that no device can access resources until the identity and authorisation can be verified is a sensible solution.

Five basic principles of a Zero Trust model:

- **Every user on a network is always assumed to be hostile**
- **External and internal threats exist on the network at all times**
- **Network locality is not sufficient for deciding trust in a network**
- **Every device, user, and network flow are authenticated and authorised**
- **Policies must be dynamic and calculated from as many sources of data as possible**

There are many reasons to employ ZTNA and as the edge/perimeter of networks become more complex, the traditional methods no longer afford the best levels of protection. In addition, the digitisation and convergence of technologies now pose new risks to organisations. Adding an always authenticate model to your security processes can provide additional security.

Copyright 2022®

01 Executive Summary

02 Introduction

03 The Growth of Cloud

04 How FourNet Can Help

Key areas of consideration for protecting the edge



SASE

A security measure growing with pace is Secure access service edge (SASE). This approach uses a framework for network architecture that brings cloud native security technologies such as SWG, CASB, ZTNA, and FWaaS

Deployed and working with wide area network (WAN) capabilities this can help to connect users, systems and endpoints securely to services wherever they are hosted.

The edge/perimeter is the gateway to your network, and as such, it needs a secure door to prevent unwanted access. Open ports and misconfigured devices leave you exposed. Often security teams are unaware of the extent of their vulnerabilities until it's too late. As the first layer in a comprehensive approach to your cyber resilience, this needs focus and attention to help build strength across your IT and security operation.

Copyright 2022®

01 Executive Summary

02 Introduction

03 The Growth of Cloud

04 How FourNet Can Help

How FourNet Can Help

Our clients benefit from our experience working with some of the biggest names in government, healthcare, and finance. We have delivered solutions that have been recognised as Best of Breed by industry bodies such as Government Digital Service (GDS).

At FourNet, we take security seriously, and our solutions are designed to strengthen security posture to mitigate threats, to protect your organisation, data and operations from downtime and breaches.

Trusted by Mission Critical Organisations

FourNet are trusted by some of the most secure and mission critical organisations in the UK, including Whitehall, Downing Street, Emergency services and other mission critical enterprises. We offer a diverse portfolio of solutions for both public sector and private enterprise with solutions including secure infrastructure, robust cloud solutions like our ANTENNA and Agile Cloud, as well as digitally transforming your customer journey.

We also provide highly available contact centre solutions delivering 999 & 111 services to the public, as well as back-office solutions to support a flexible, agile workforce and have highly accredited and security cleared engineers and consultants.

Helping You to Understand Security Posture

FourNet's Security Specialists are here to help your organisation detect, defend, and repel threats from whatever threat vector they emerge. Our team of experts will work alongside you to identify and remediate areas of concern or risk. We work with you to build a business case to demonstrate ROI and payback periods based on your current costs and KPIs. Get in touch to schedule an initial discovery call.

Managed Security to Remove the Worries

We offer a range of managed solutions from the world's leading security vendors all underpinned by SC and DV level security cleared engineers and consultants. Our best-in-class security cleared service management from our dedicated secure Service Desk, FourNet provides a fully managed service desk and Security Operations Centre (SOC) with 24/7 phone support and multi-factor authenticated ITSM access.

Whether you are looking to secure your edge or SD-WAN infrastructure, or simply looking to control access to critical systems and data, we can help. We work with you to understand your organisation, network and operations and provide the help, solutions, and support where it is needed most and can deliver the best outcome.

Discover how robust your cyber defences are – Get started with a Fortinet Cyber Threat Assesment

Our Fortinet Cyber Threat Assesment Audit (CTAP) gives customers an in-depth view of the current state of their security. We offer CTAP to help identify strengths and weaknesses across your organisation, highlighting vulnerabilities that require attention.

Using a CTAP gives organisations a clear and defined list of actionable areas to improve and protect data, network, and staff.

Copyright 2022®

FourNet®

Manchester Office (HQ)
3 Scholar Green Road,
Cobra Court,
Manchester. M32 0TR
Tel: 0845 055 6366

London Office
83 Victoria Street,
London. SW1H OHW
Tel: 0203 503 0003

Burton Office
First Floor, Unit 10 Barberry Court,
Burton-on-Trent,
Staffordshire. DE14 2UE
Tel: 01283 519020

Scarborough Office
Unit 2, Lora Court
Wykeham Business Centre
Scarborough,
YO13 9QP
Tel: 0333 344 8971

FourNet PR & Media Office
Tim Reid
e-mail: treid@fournet.co.uk

0161 864 5130
sales@fournet.co.uk
www.fournet.co.uk

Copyright 2022®