Network security fundamentals

How to design, use, and maintain secure networks.

Networks are fundamental to the operation, security and resilience of many organisations. This guidance provides an introduction to the key topics to consider when designing, maintaining, or using networks that need to be secure and resilient. It will also help you apply the NCSC's Cyber security design principles to networks. More technical information is provided in the 'further reading' sections.

> **Note**
> While some topics covered here are relevant to cloud-based networks, you should refer to the NCSC's Cloud security guidance for specific information about cloud-based networks.

Identifying your Assets

Do you know what assets your network is made up of?

Identifying **all** the assets that make up your network is a key step towards security and resilience. A common way that an attacker can gain access to a victim's network is through systems on the network that the organisation is not aware of, and therefore are not secured (or decommissioned) appropriately.

Further NCSC reading:

Asset management guidance
Implementing asset management for good cyber security.

Acquiring, managing, and disposing of network devices

Guidance for organisations on the acquisition, management and disposal of network devices.

Products on your perimeter considered harmful (until proven otherwise)

A blog describing how attackers infiltrate into networks through internet-reachable products.

Understanding the threat

What threats do you need to be protected against?

The controls you incorporate into your network should align with the specific threats you need to guard against. If you don't perform 'threat modelling', it is highly likely you will waste resources implementing controls against irrelevant threats (or even worse, leaving your network vulnerable to unrecognised threats).

Further NCSC reading

Threat Modelling Guidance

How threat modelling can help inform risk management decisions.

Restricting access

How do you restrict access to your network to only the people and systems you want?

Access to your network and the assets within it should be controlled. The principle of 'least privilege' should be followed and means users and systems have access only to the resources needed to do their job.

Further NCSC reading

Minimise the privilege and reach of applications
Guidance on how to choose, configure and use devices securely.

Enterprise authentication policy guidance
Implementing effective authentication on smartphones, tablets, laptops and desktop PCs.

Systems administration architectures
Guidance on some common approaches to system administration architectures.

Systems administration

Highly privileged accounts, like those used for system administration, are prime targets for attackers. Administrators can typically change security settings, install software, delete users, and access all files on the computer and administrator access provides the high level privileges required to make these changes. For this reason they should be secured proportionately to the risk they pose to the organisation should one of these accounts be compromised.

Further NCSC reading

Secure system administration guidance
Design principles that can help to protect your most sensitive data.

Security architecture anti-patterns
Design patterns to avoid when designing computer systems.

Passwords and PINS

Passwords and PINs allow users to prove their identity to gain access to a network. Passwords and PINs should be used alongside additional authentication factors to enhance security through multi-factor authentication (MFA).

Further NCSC reading

Multi-factor authentication for your corporate online
Advice for organisations on implementing strong methods of MFA.

Authentication methods: choosing the right type

Recommended authentication models for organisations looking to move 'beyond passwords'.

Password administration for system owners

Password strategies that can help your organisation remain secure.

Allow lists and deny lists

Allow lists and deny lists help you to control access to resources, including networks. **Allow lists** will only permit specified access to a resource, whilst **deny lists** will only block specified access. If you want to uphold the principle of 'least privilege', you should use allow lists. Deny lists can have significant limitations as they can only deny what is known about and included on the list, which means attackers may be able to access a resource that is not excluded.

Certificates

Certificates are normally a more robust method for authentication when compared with other mechanisms (such as passwords) . However, they can be more difficult to implement and maintain. Examples of where certificates can be used are for network access, Transport Layer Security (TLS) and Virtual Private Networks (VPNs).

Further NCSC reading

Using Transport Layer Security to protect data

Recommended profiles to securely configure TLS.

Virtual Private Networks

Choosing, deploying and configuring VPN technologies.

Designing network architecture

Has security and resilience been designed into your network from the start?

Identifying and implementing the most appropriate network architecture can:

- help to make compromise and disruption by an attacker more difficult
- reduce the impact of a compromise should one occur
- make it easier to detect potentially malicious activity

If security and resilience are not incorporated in the design stage, it can lead to greater difficulties (and costs) later on.

Further NCSC reading

10 Steps To Cyber Security: Architecture and configuration
Design, build, maintain and manage systems securely.

Device security guidance: network architectures
Advice on designing a remote access architecture for enterprise services.

Secure design principles
Guidance on the design of cyber secure systems.

Network segmentation

Network segmentation is all about breaking your network down into smaller networks. This allows you to control how traffic flows, and what access is allowed between these different networks. Segmentation should also be considered when determining how the management interfaces (used by administrators to configure your infrastructure) can be protected.

Further reading

Preventing Lateral Movement
NCSC guidance for preventing lateral movement in enterprise networks.

Implementing Network Segmentation and Segregation
Guidance from the Australian Cyber Security Centre.

Zero trust architecture

A zero trust architecture is an approach to system design where inherent trust in the network is removed. Instead, your network is assumed hostile and each access request is verified, based on an access policy. Confidence in the

trustworthiness of a request is achieved by building context, which in turn relies upon strong authentication, authorisation, device health, and value of the data being accessed.

Further reading

NCSC's zero trust architecture design principles
How to implement your own zero trust network architecture in an enterprise environment.

NIST Zero Trust Architecture (PDF)
Advanced guidance from the US National Institute of Standards and Technology.

Protecting data in transit

How do you protect data that traverses networks?

A primary function of a network is to be able to move data around it. This may mean that sensitive data passes across devices whose security cannot be assured. Due to this, it is important you put controls in place to protect the confidentiality, integrity and availability of data in transit.

Virtual private networks (VPNs)

How do you secure access and connections from outside of your controlled network?

VPNs are a way to create a secure network connection over an untrusted network. It is imperative that if VPNs are used the software and appliances that implement them are maintained appropriately throughout their entire lifecycle and not just forgotten about once implemented. If this is not done, you increase the likelihood of critical vulnerabilities being exploited by attackers, giving them a foothold in your network.

Further reading

Device Security Guidance: Virtual Private Networks
NCSC's guide to choosing, deploying and configuring VPN technologies.

Zero trust migration: How will I know if I can remove my VPN?

An NCSC blog that considers the security properties of an 'Always On VPN'.

Protocols

Are the protocols you use appropriate?

The protocols supported by your network should make compromise and disruption difficult. Should a compromise happen, this can be easier to detect and the impact reduced if the protocols chosen have been done so with security and resilience in mind. Choosing protocols with security benefits built in is beneficial over choosing protocols without. For example if you are hosting a website you should look to use HTTPS over HTTP.

Further NCSC reading

Using Transport Layer Security to protect data

Recommended profiles to securely configure TLS.

Protocol Design Principles

An NCSC paper aimed at designers of protocols, as a guide for use in the design process.

Securing network perimeters

How do you control what you allow in and out of your network?

Even though identifying network boundaries can be challenging, especially with the adoption of zero trust architecture, protecting known network boundaries remains crucial. The boundaries between different subnets or security zones are examples of where perimeter security should be enforced. A common way to do this and control what is allowed to cross a perimeter is through the use of firewalls. It is becoming more common to take steps to carefully manage and protect Domain Name System (DNS).

Further NCSC reading

Products on your perimeter considered harmful (until proven otherwise)

An NCSC blog examining how attackers' tactics have changed to infiltrate networks.

Firewalls and allow rules/deny rules

Firewalls can be hardware or software-based, and are used to prevent unauthorised access to or from a network. Firewalls come in various types from simple packet-filtering firewalls through to 'next generation' firewalls (which combine simple packet filtering with other functions that filter data at the application, rather than transport layer). One thing all firewalls have in common is their use of allow and deny rules.

- **allow rules** control access to a network or system by only allowing through traffic that matches a predetermined set of attributes (such as source or destination IPs, domains, ports or applications amongst other attributes)
- **deny rules** work in the opposite way by only denying traffic that matches a pre-determined set of attributes such as a list of known malicious IPs or URLs

Firewalls will most likely use a combination of allow and deny rules called rule sets. These rules tend to be processed in a top-to-bottom priority order, with the first match (either an allow or deny rule) being the one that is followed. Implementing a final 'deny all' rule after setting up rules that permit access, only to the minimum necessary resources is good practice to uphold the principle of least privilege.

DNS

Almost all networks rely on DNS to some degree so securing this is critical. You may have your own DNS servers resolving human-readable queries into IP addresses that computers understand, or your may rely on DNS servers that are not under your control. Whatever the case, there are protections that you should put in place to combat the threats to DNS. These include, but are not limited to:

- controlling who can make changes to your DNS record and/or server
- limiting the amount of DNS queries that can be made

- protecting the queries themselves by using DNS Security Extensions (DNSSEC)
- Implementing a deny list of known bad domains from an appropriate threat intelligence feed

Further NCSC reading

Protective Domain Name Service (PDNS)

About the NCSC's PDNS service, designed to hamper the use of DNS for malware distribution and operation.

Protective DNS for the private sector

Advice on the selection and deployment of Protective Domain Name Systems (DNS).

PDNS for Schools

The NCSC's 'Protective Domain Name Service for Schools' scaled-up to protect a wider range of organisations.

Managing Public Domain Names

Good practices for the management of public domain names owned by your organisation.

Updating systems

How do you keep your systems secure and up to date?

Installing the latest updates is critical to ensuring the security of your estate. You should put in place a policy to update by default, where you always apply updates as soon as possible, and ideally automatically. This should be at the core of your update management process as the desired standard for systems, but it may not apply in some circumstances (such as for safety-critical systems or operational technology). Systems that are not regularly updated may contain vulnerabilities which are widely known about. Attackers may be able to easily exploit these to gain a foothold on your network.

Further NCSC reading

Vulnerability management guidance

Principles to help organisations establish an effective vulnerability management process.

Monitoring networks

How do you detect if your network has been compromised?

By having an effective security monitoring function, your organisation will be able to identify any activities that are taking place on your network that are not in accordance with your organisation's policies or expected behaviour. This enables swift detection and remediation of threats before they can cause excess harm. When creating or reviewing your security monitoring function, it's important that you:

- understand what you are monitoring for
- ensure the necessary logs are available for analysis
- ensure your analysis provides useful insights
- ensure you can detect signs of misuse

Further NCSC reading

Logging and protective monitoring guidance

Using logging and monitoring to identify threats and protect devices.

Building a Security Operations Centre

Guidance to help organisations design a SOC and security monitoring capability.

To SOC or not to SOC ?

A blog explaining that for environments that are 'secure by design', a 'full-fat SOC' is not always required.

PUBLISHED

6 February 2025

REVIEWED

6 February 2025

VERSION

1.0

WRITTEN FOR

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals