ambersail

THE IMPORTANCE OF NETWORK SEGMENTATION

Ben Sandison. Penetration Tester, Ambersail Ltd.

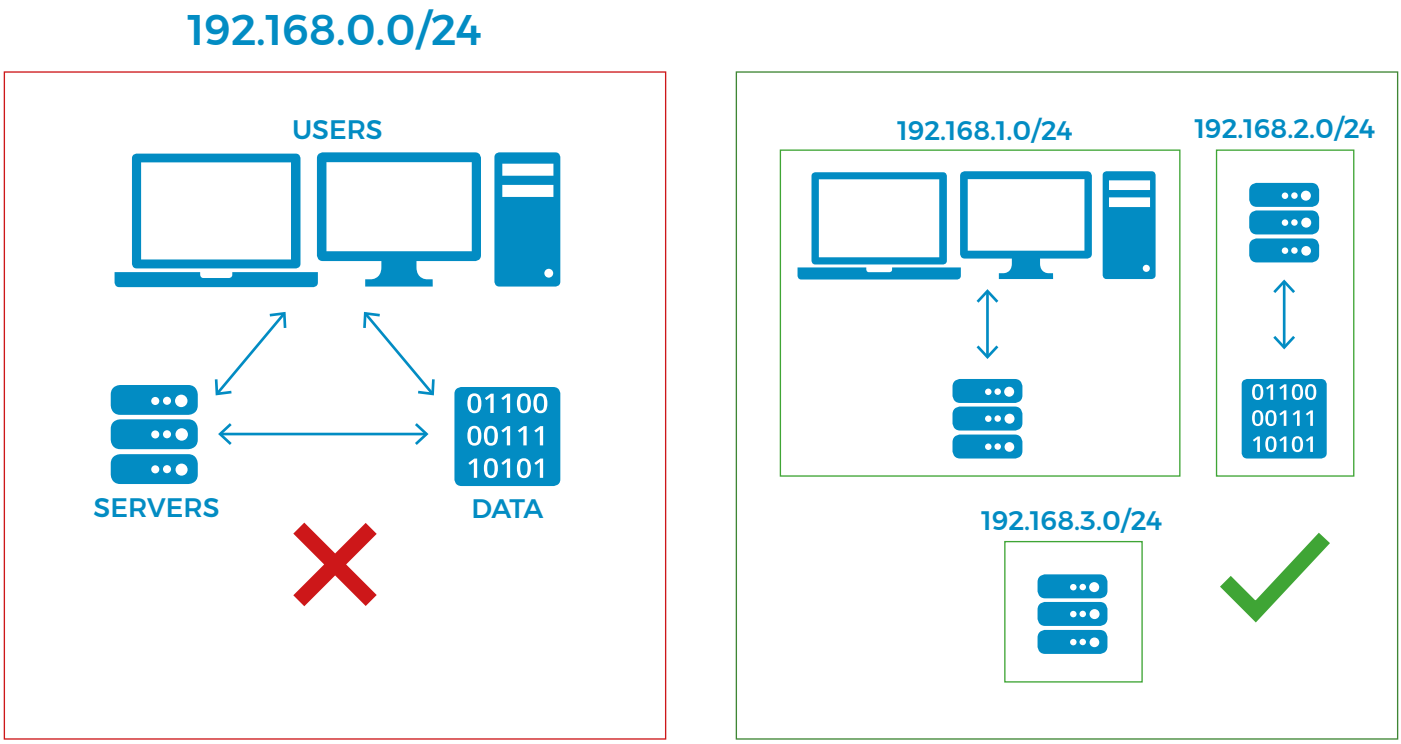
READ OUR SHORT GUIDE ON NETWORK SEGMENTATION

WHAT IS NETWORK SEGMENTATION?

Network segmentation is the method by which a large, flat network can be divided into a number of smaller ones.

This segmentation can be done in numerous ways, physically or virtually. The goal often being to restrict access to sensitive network devices and services to only those who need them.

This can make administration of the network more complex. Network administrators will need to be able to access each of the new network segments individually, without introducing entry methods which an attacker could abuse to defeat the protections in place. That is why careful planning is important.



www.ambersail.com | enquiries@ambersail.com | +44 (0)1925 607250

WHY IS NETWORK SEGMENTATION IMPORTANT?

BUSINESS CONTINUITY

From a business perspective, network segmentation provides numerous benefits. Logical separation of internet-facing and sensitive internal systems allows simpler management of data and services. This separation also ensures that should a network disruption occur only part of the business will be affected, allowing the rest to continue as normal.

AUDITING

Segmentation also allows easier auditing, whether it be for security, peace-of-mind or for compliance purposes. For example, PCI DSS and **Cyber Essentials** both can take advantage of network segmentation, allowing the scope to be reduced and making compliance much simpler to achieve.

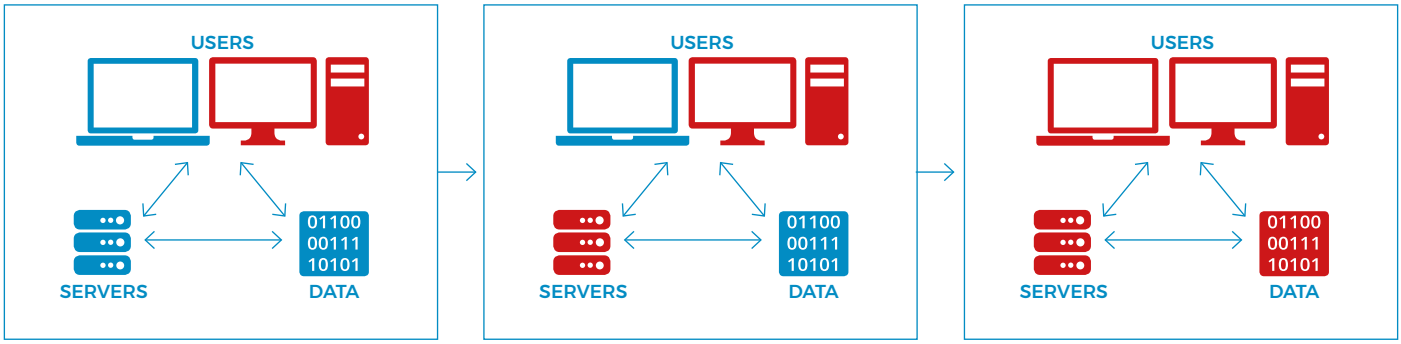
SECURITY

In terms of security, network segmentation heavily reduces the risk of a significant security breach.

An attacker (or a penetration tester) with access to a flat network will actively search for ways to achieve 'lateral movement'. This is the process by which an attacker with access to one machine on a network moves laterally across it, infecting every other machine on the same network.

At Ambersail we regularly take advantage of this during penetration tests, taking full control of networks from a single starting point.

When implemented correctly, the most sensitive data and business-critical services will be on network segments with the strictest security boundary. Should an attacker gain access to any other segment they will find it significantly more difficult, if not impossible, to gain access to the assets considered most important.



WHERE DO I BEGIN?

The key to effective network segmentation is the time spent planning and designing the new network layout. Full awareness of all digital assets and who needs access to them is critical in ensuring the exercise is not wasted time.

1 ASSET DISCOVERY

The first stage can be the most straightforward but may well take the longest. Asset discovery involves creating a full list of everything on the network which either needs to be accessed or needs access to something else. A complete list is likely to include devices, services, data stores, virtual servers and last but certainly not least: people.

The granularity of the list is critical for future planning. It may be that you have a single data store for use by IT, HR and sales staff. It is important that these would be considered separate, as this allows the greatest flexibility when moving to the grouping stage.

STAFF
SERVERS
DATABASES

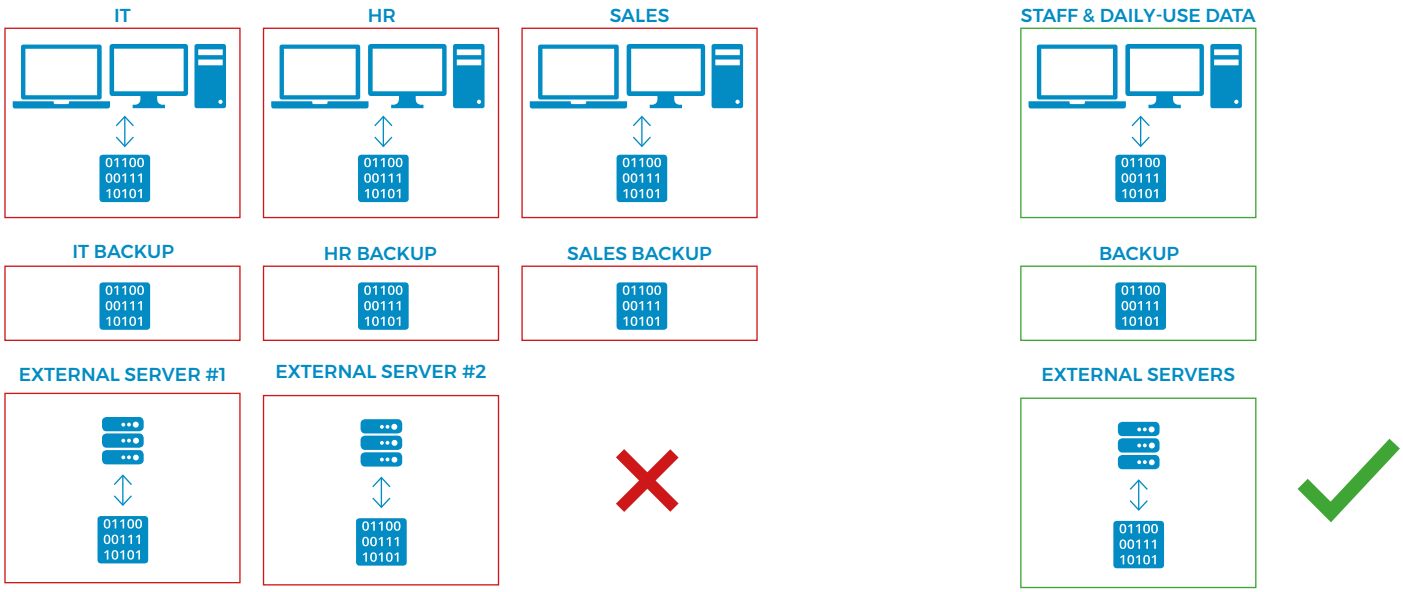
HR STAFF
IT STAFF
WEB SERVER #1
WEB SERVER #2
INTERNAL SERVER #1
HR FILE SHARE
SALES FILE SHARE
SALES PRINTER
CRITICAL DATABASE
BACKUP DATABASE

2 GROUPING

The second stage involves taking the list of assets and determining any links between them. From this relationship, logical groups can be drawn. These groups will form the basis for individual network segments.

To begin, these groups should be made fairly broad. If starting from a flat network, attempting to immediately move to a fully segmented one is likely to cause significant business continuity issues. This may leave the network in a worse state than it was originally due to complex but incomplete rules.

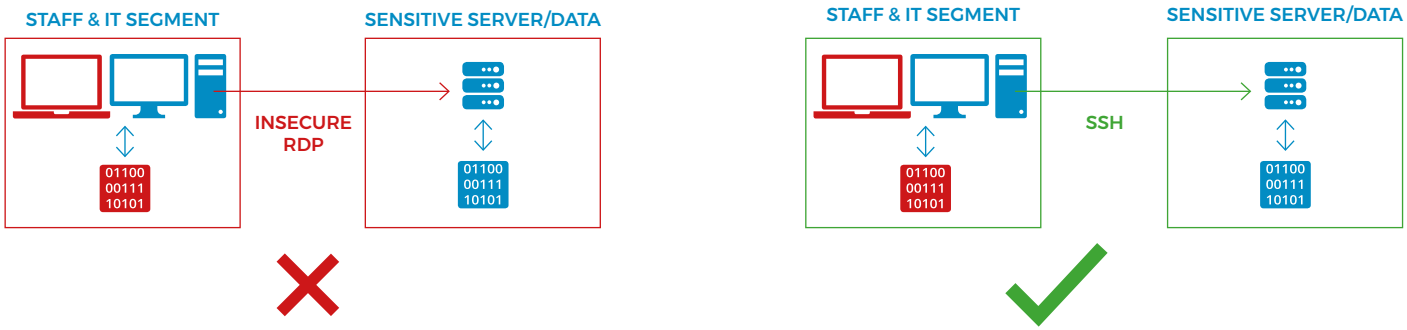
Typical groups for initial segmentation include: Internet-facing hosts, a DMZ, and an internal network. A fourth group containing critical data that does not need regular access could also be created, if it fits the business need. Other frameworks exist for this stage, but it's important to use one that fits.



3 IMPLEMENTATION

The final (and ongoing) stage is to implement the design from above. There are numerous options for going about this, but the two most common involve either physically separating the network segments or implementing Virtual LANs (VLANs) with network Access Control Lists (ACLs).

Of course, it is necessary for network administrators to be able to cross these boundaries. Implementing mechanisms to do so needs to be considered before cutting off traffic flow. Commonly this will involve highly secured remote access protocols such as SSH being in-use, or the use of a hardened bastion host known as a 'jump box'. **Bear in mind that should remote access not be secure enough an attacker may take advantage of it in order hop between network segments.**



It is often helpful to deploy the implementation in stages. This helps reduce the risk of significant network disruption affecting business operations.

COMMON PITFALLS

Network segmentation provides a multitude of benefits when executed properly and treated as a continuous exercise. It is important however, not to jump in too quickly.

Proper planning and a phased release schedule are critical. Moving from a flat network to a fully segmented one overnight is likely to cause significant business continuity issues. This may involve various elements of the business being unable to access services that they need to, or in the worst case, confusion leading to data loss.

Users are not likely to react well to many large changes at once, and in most cases will attempt to circumvent the restrictions in place. This can significantly reduce the effectiveness of the solution.

IN CONCLUSION...

Network segmentation is a great way to introduce security measures which, after the initial setup is over, are effectively transparent. True segmentation can help prevent attackers spreading, can improve performance and can even make life easier during external audits.

Planning is the key to success. But the final thing to remember is that this is not a one-off. Network segmentation is a continuing strategy which must react to changes in the network and the wider Internet. Otherwise the network will become an ever more complex and unmanageable beast, with as much vulnerability as any flat network.