Infrastructure Solutions International whitepaper

Enterprise Mobility:
Securing the network perimeter

Introduction

Defining the network perimeter is as complex as ever. It's safe to say that mobility has changed the architecture and design of the network. As organizations increase the use of mobile technologies to remain competitive and to enhance employee productivity, the network needs to handle a surge in a variety of traffic in a secure way.

The network infrastructure that an organization has in place today typically does not meet their mobility needs. The expertise in understanding mobility challenges and providing the appropriate solutions is something that few organizations do right. The intent of this whitepaper is to help you align your network to support your mobile initiatives.

Market Drivers

Mobility is a unique task given that requires security at all levels. The market for mobility has changed the requirements for a network. Enterprises of all sizes are dealing with these changes, as some are starting from scratch while others are moving from a line of business-focused to an enterprise-focused strategy. Regardless of where you are, the mobility landscape is pushing organizations to upgrade their network to ensure its mobile ready.

- Mobility management includes everything from applications, devices, data, and so one. Whether there is an established vendor or new vendor, there are many approaches to managing mobility. With so many approaches due diligence needs to be taken to assess which approach supports your needs. However, we see lifecycle issues that make a mobile strategy a moving target.
- Network Traffic has increased and will continue to increase due to your mobility. Cellular service providers are doing what they can to keep up with the demand. WLAN vendors are also working hard to ensure the latest technology supports mobile initiatives. A reliable connection is key to mobile-first enterprise.
- Network Security in a mobile environment that manages both insider and outsider threats has become a challenge. The threat vector has changed and become more sophisticated. If an organization doesn't know how valuable their data is or who their users are, it then becomes an uphill battle to secure the network.

Difficulties in securing the network perimeter

1. Tunneling

   Tunneling has been used for years to provide remote users access to corporate resources. Prior to enterprise mobility, the organizations typically used SSL or IPSec VPNs. Now with the broader adoption of mobile platforms new tunneling solutions are beginning to emerge, such as Per-App Container/Device/User VPN and enterprise mobility management (EMM) tunnel. Investments have already been made in previous technology, which leads to questioning of which solution is right for us.

   - SSL VPN –corporate access using a web browser.
   - IPSec – corporate access that requires a client application on the device.
   - Per-App/Container/Device/User – corporate access based on specific application, container, device or user.
   - EMM Tunnel – corporate access without deploying a VPN.

2. Access to the enterprise

   Access to the enterprise is being given to a growing number of users. They have access at any time and from anywhere. Some organizations even go down the path of giving users access to everything and then lock it down at a later date. With mobility changing rapidly organizations use this approach to handle the unknowns. The problem is that date never comes, and the attackers have open access to steal anything they want.

   Besides users access, application and device controls need to be put in place to control access. The standard authentication, authorization, accounting (AAA) framework needs to be used to ensure the network isn't putting users at risk.

3. Wireless security

   Cellular and WLAN play an important role in securing the network perimeter. Typically with cellular the risk is transferred to the mobile service provider. As an organization, you have more control over the WLAN security that is in place.

   The WLAN needs to be viewed from both an internal and external perspective. Internally an organization needs to understand their applications, devices, and users that are on the traversing their networks. The issue is that typically organizations haven't aligned those three areas together to generate the right WLAN policy.

   External WLANS is where users put their organizations at risk, without knowing it. The ability access the internet via a hotspot, hotel, convention center, and so forth can expose a security domain that organizations don't control. Sometimes WLAN coverage is better than cellular coverage in a certain area. The typical scenario is for your users to access a WLAN and complete a task. However the how do you know if a user is using a rouge Access Point (AP) to access corporate resources? Now organizations are left trying to frame a wireless security problem that is broad and complex to control.

Aligning the network infrastructure to support mobility

Understanding that the network in mobile enterprise is a large system, that consists of multiple components that move in an out of and organization's mobile security domain. There is a need to break the system down into its components or subsystems. Within each component, evaluate what you need to control. The way to think about that is "How can we prevent a data breach". Then next do a gap analysis what you have in place now. This will show you where need to make investments.

The goal at the end of the day is focused on managing risks by aligning the network to your mobility initiatives. Defining the perimeter in terms of Users -> Devices ->Applications -> Data, puts into context how a business can structure the network to support enterprise mobility.

In order to secure the mobile perimeter evaluate these five areas of your network.

1. Network Segmentation – A layered approach requires classifying the networks. Then you need to ensure traffic is blocked to applications and data that haven't been associated with the enterprise mobility domain.
2. Connectivity – Understand the various network connection options that a user has. Then determine how you can control the connections. Some options are to control connections with access time schedules, managing persistent connections, and so forth.
3. Firewall - If your firewall is using legacy capabilities of source/destination IP address and ports, it time for a technology refresh. The features in a next-generation firewall (NGFW) allows organizations to get granular with network traffic by adding user access controls, packet inspection, network application/ID control, intrusion detection system/intrusion detection systems (IDS/IPS), traffic inspection and more to legacy firewall capabilities.
4. Network Access Control (NAC) – The NAC give an organization the ability to make network decisions based on device visibility. The ability to align the device application posture to your network access control.
5. Tunneling – within a mobile enterprise resources are available anytime and anywhere. There are options when it comes to allowing the access. Understanding your data will determine which approach is best for the business.

Conclusion

Mobility has changed how organizations secure the network perimeter. More than ever a layered approach is needed to ensure all mobility risks are managed appropriately. Ideally having end-to-end access controls in place that align to user's roles and responsibilities will help manage the mobility risks. If an organization can effectively protect corporate data, they are able to quickly audit their security posture and adapt quickly to mobile changes. As technology continues to move towards anytime/anywhere access organizations need to ensure the network is up to the challenge. The value in the network is being able to analyze that information traversing it. If it's secure, then an organization can maneuver quickly to realize new opportunities that support their mobile initiatives.

About us

Infrastructure Solutions International is a mobility and wireless solutions provider. With technical staff experienced in cloud, networking, mobility, security, and wireless we have the expertise to solve your problems.

Infrastructure Solutions International
www.infra-si.com
info@infra-si.com