Basis Networks

# Achieving a Future State Architecture: The 5 core steps

basis networks

# Contents


Introduction 3

Future state change model 4

Balancing trade-offs in your Future State Reference Architecture 5

Finding the balance 7

Building the roadmap to your future state 8

REFERENCE ARCHITECTURES EXAMPLE #1
Security as the core focus 9

REFERENCE ARCHITECTURES EXAMPLE #2
Agility without compromising on security 11

Conclusion 13

ACHIEVING YOUR FUTURE STATE

# Introduction

In the context of IT networking, the term Future State Architecture seems fairly self-explanatory. As Gartner said back in 2017, "The future-state network is an aspirational view of how enterprise network architectures should evolve….". Evolution has always been a part of a network's DNA and we know networks will keep evolving as business requirements change and new technologies emerge.

The challenge is to ensure that this evolution is as planned as possible and happens in a structured, deliberate way to ensure it aligns to the second part of the Gartner definition. "…to meet emerging business requirements and be more closely aligned with critical business objectives."

This is the critical point. A future state architecture must align to the business and what it needs to be successful in future, not invest in technology for technology's sake. The architecture must serve the business.

The challenge in this is in understanding what the business will actually need. As digital transformation initiatives gather momentum and next-gen technologies, fuelled by advances in AI and 5G take hold, it's never been harder to predict what an enterprise will demand of their networks in 3, 4 or more years' time.

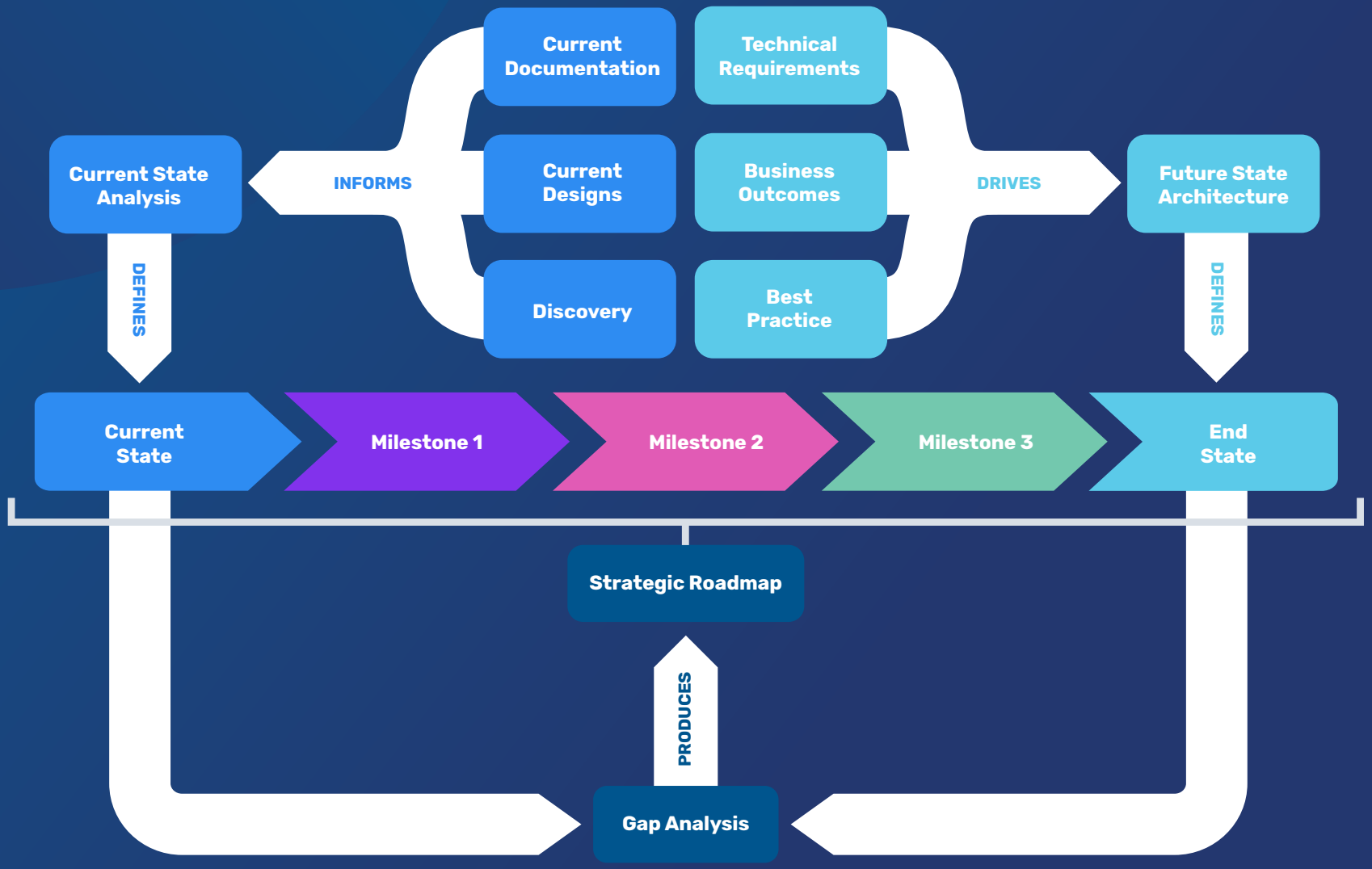
Anecdotally, we have seen this challenge lead to more short term thinking with companies adopting more incremental change rather than bold visions of change. If you consider the way cloud services have been adopted and the resulting distributed nature of customers, applications, and data, you can see the result of this shorter timeframe thinking with networks architectures that have become unnecessarily complex, expensive, inflexible and insecure. They're often incapable of supporting the changing approaches to business that they were supposed to cater for.

As a result, we believe it has never been more important to take a more formal and structured approach to the evolution of the network – a Future State Architecture approach.

In this paper, we'll focus on how to define that desired future state, while still ensuring alignment with business drivers. We'll look at the trade-offs between competing objectives and provide two example reference architectures that are each optimised for specific business drivers.

FUTURE STATE ARCHITECTURE FRAMEWORK

# Future state change model



FUTURE STATE ARCHITECTURE FRAMEWORK

# Balancing trade-offs in your Future State Architecture

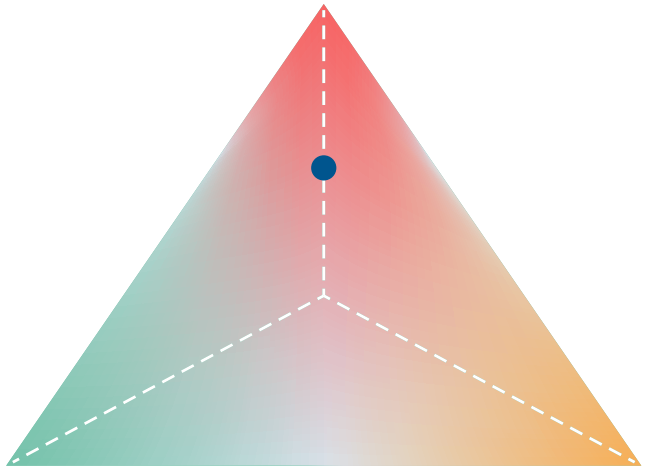
There is obviously no single “best-practice” reference architecture that an enterprise can use to guide their efforts in defining a future state. Instead there are a series of trade-offs based around three fundamental assumptions, or problems, about the network that any reference architecture needs to consider:

- The network is insecure
- The network is expensive
- The network is incapable and inflexible.

The challenge is that a focus on optimising for any one of these problems in any future state reference architecture often requires a level of compromise in at least one (if not both) of the other two. For example, a reference architecture that puts a high focus on security, can struggle to also be highly agile and low in cost as can be seen in this diagram.

## Security

As companies collect more customer data and distribute data stores and workloads across a variety of locations which are accessed by people on different platforms via different methods, security becomes harder to accomplish. Add to this, the constant evolution of the threat landscape which has significantly impacted the effectiveness of traditional ways of securing the network.



## Cost effective

The adoption of cloud services, and the distribution of data, applications, and customers, has resulted in network and security architectures that are overly complex, and typically built from multiple platforms with overlapping capabilities. This complexity results in significant cost for both operations and any projects which require changes to the architecture.

**OUTCOME WEIGHTING**

## Agility

Traditional network and security technologies are not optimal for the delivery of the rapid changes required to support digital initiatives. Additionally these technologies do not typically facilitate the type of insight required to identify and improve the end-user-experience.

**Ultimately, you need to find the right balance between each of these dimensions, aligning your focus with your business drivers and priorities.**

| | OPTIMISING FOR Agility | OPTIMISING FOR Security | OPTIMISING FOR Cost |
|---|---|---|---|
| **Potential Drivers** | • Businesses that must adapt in a digital marketplace.<br>• Businesses that differentiate based on exceptional user experiences and the need to constantly add new features and capabilities to their products and services.<br>• Businesses that search for best-of-breed solutions to their business problems. | • Businesses needing to protect highly sensitive data.<br>• Businesses with specific regulatory or data sovereignty requirements.<br>• Businesses providing critical services with high availability demands i.e. needing 100% uptime. | • Cost is always a factor for any business, but cost reduction isn't always about the bottom line. It can include OPEX and CAPEX trade-offs, Total Cost of Ownership considerations, or soft costs such as time saved. |
| **Outcomes** | • A robust architecture that is easy to consume and adapt to your need. i.e. cloud-like. | • Much easier to establish continuous compliance with automation and centralised configuration management.<br>• An architecture with increased resilience, uptime and compliance.<br>• Low risk of data loss. | • An architecture that relies more on automation to lower operational overhead.<br>• An architecture that is designed to use cheaper cloud services easily through workload mobility. |
| **Trade-Offs** | • Agility can be expensive and complex to maintain.<br>• Limited tooling is a challenge.<br>• Security may lag behind the adoption of new functions or capabilities which presents an increased risk. | • Agility is hard to manage with considerable time required to thoroughly vet any changes to understand the impact of the change on the level of security.<br>• Maintaining such high levels of security and/or uptime can be difficult to automate resulting in more expensive, high effort-based approaches to ensure consistency across the network.<br>• Multiple clouds make this even more difficult with some cloud functions or services completely ruled out. | • As already noted, optimising for agility and security can be expensive so focusing on costs often means accepting lower levels of security and less agile infrastructure.<br>• Your customers may not be happy with the performance or user experience your network provides. |

A REAL WORLD EXAMPLE

# Finding the balance

**In defining a future state architecture, we often look to define the core capabilities in each of the above problem areas, expressed here as directives. These directives then guide the gap analysis phase as you evaluate your current state network against each directive.**

**If we consider a scenario where an enterprise is optimising for security:**

| OBJECTIVE | LOWER SECURITY RISK | COST REDUCTION AND SIMPLIFICATION | IMPROVED AGILITY AND CAPABILITY |
|---|---|---|---|
| IMPORTANCE | • High – The improvement of the enterprise network security posture is the primary driver for the enterprise. | • Medium – While this is highly desirable, the need for security will override cost reduction and simplification factors when making architectural decisions. | • Low – These benefits are not directly mandated outcomes for the architecture. While the ability to deliver these objectives is still beneficial, they're not a critical set of outcomes. |
| DIRECTIVES | • Risk reduction is largely predicated on the improvement of security and visibility throughout the enterprise. These need to be fundamental considerations within the architecture.<br>• The reference architecture must also account for any regulatory and compliance requirements that the enterprise is subject to.<br>• The architecture should propose a modern security paradigm that allows for a much more effective mechanism by which to secure complex, distributed networks.<br>• The solution should allow the much more granular application of controls based on the different data security needs by defining internal micro-segmentation.<br>• Network intelligence is fundamental to the effective delivery of enterprise wide security and must be examined as part of the architecture. | • Several cost reduction mechanisms can be examined as part of the architecture and included if they are deemed appropriate.<br>• These include directives such as platform consolidation and any potential for a reduction in vendor sprawl.<br>• Any recommendations to purchase new infrastructure must consider the cost of operations and ensure that platforms are suitably elastic and scalable to cost-effectively deliver both present day and future networking requirements.<br>• Consideration of platform automation capabilities and integration into orchestration platforms must also be examined, to allow the enterprise to manage larger, more complicated networks more effectively. | • Capability augmentation can improve the ability of the network to effectively service both external consumers as well as internal users.<br>• One of the aims could be to allow the business to more effectively engage with existing customers, as well as to obtain new customers.<br>• The other tenet of capability improvement is to allow internal users to more productively use the network, whether this is through improved remote access, BYOD, or any number of other modern work convenience directives.<br>• The experience you deliver should be ingrained in the network automation, which is fundamental aspect of the reference architecture. |

# Building the roadmap to your future state

After working through the above steps, you should now have a clear picture of the desired future state. Completing the gap analysis then ensures clarity of the starting point while also providing a way to measure how much work is needed to get to that future state architecture. Now we need to determine the right steps to take along with the timing to get there.

While this can be just as challenging as the other steps, there are several directives that can help advance a network or security to the desired state. This can include things such as simple replacement of legacy switching platforms with newer, more capable alternatives or perhaps introducing segmentation into the network to improve security.

The most challenging aspect of creating a roadmap is managing priorities – what should you do first?

**Analysis of the costs and benefits of the two directives is critical here. This generally involves asking risk-based questions such as:**

- What is the risk of not introducing segmentation into the network and having private or critical data stolen by hackers?
- What is the risk of these old switches failing, and as a result the business losing access to hosted applications?

Quantification of the risks associated with these decisions is preferable as this allows a direct comparison between them to determine which directive will have the most immediate benefit. Quantitative risk assessment also formalises the thought process by encouraging decision making to consider aspects around the impact of the suggested changes.

- What is the impact of losing access to hosted applications?
  - Is it just productivity?
  - Do we stand to lose customers, or are these applications merely for internal use?
- What is the impact of having critical data stolen?
  - Is there a legal obligation to disclose this?
  - What will the reputational impact be?
  - Are we financially liable?
  - What kind of costs could this incur?

This enriches the decision-making process by allowing more points of comparison between the two directives. The process of doing this comprehensively across the full set of roadmap directives will help establish the overall sequence of each step.

REFERENCE ARCHITECTURES EXAMPLE #1

# Security

## Background

This enterprise has a government mandate to supply a critical service to the nation. As part of achieving this, they are required to collect sensitive information that must be kept extremely secure. The enterprise only services a single country and growth and expansion are negligible. It offers minimal consumer interaction, and the requirements are not sophisticated.

Costs are not generally a concern, but the business sells a critical product, and has an ethical requirement to ensure that costs are controlled. As part of this, the business has flagged potential ways to reduce costs:

- Move to cloud
- Network automation
- Automation of manufacturing processes which has resulted in an increased adoption of OT and IoT.

The business has a large onsite footprint due to the real-world nature of the work.

## Solution

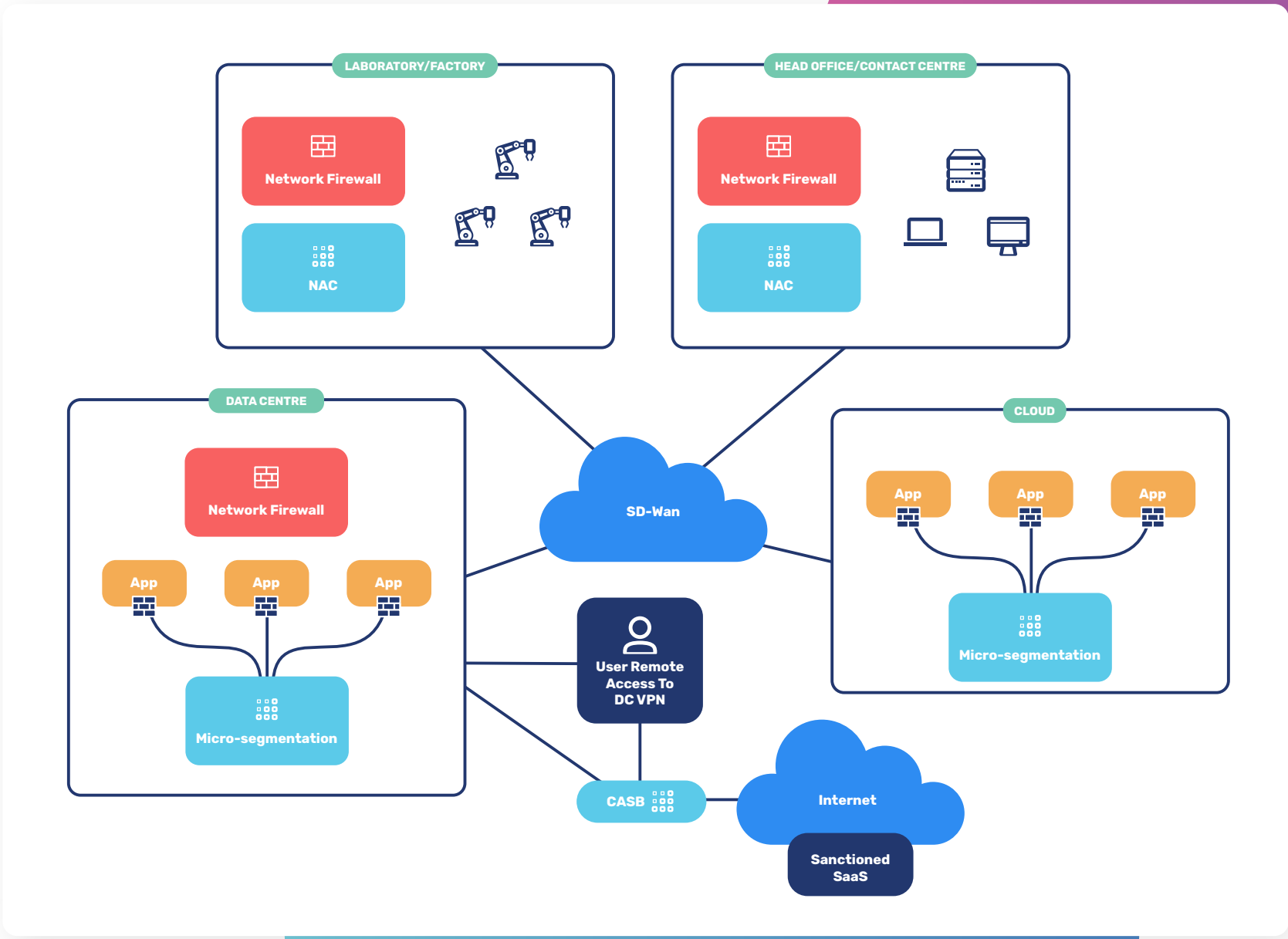
When considering an architecture for such a business, these aspects all have to be considered, and steer the architecture in a particular direction.

The reference architecture will cover:

1. **A new data centre network that must be easy to operate and can be automated**
   a. This will deploy a centrally controlled data center fabric
   b. Early investment in automation will drive down ongoing operational costs
   c. Eventual evolution of the fabric to IaC will make consumption even easier
2. **Connectivity for the various facility types must cater to everything from users to IoT infrastructure**
   a. This will require both secure LAN and Wi-Fi for user facilities
   b. Security of IoT
   c. Both require a highly capable NAC solution
3. **Secure connectivity to cloud or multi-cloud**
   a. Multi-cloud or secure access to IaaS and SaaS is required
4. **A consistent application and view of security across the enterprise**
   a. Controls include
      i. Firewall macro-segmentation in the data centres (and possibly in the cloud)
      ii. Agent-based micro-segmentation for both cloud and DC
   b. This must account for the various atomic controls and offer a unified view and application of security

REFERENCE ARCHITECTURES EXAMPLE #1

# Security (cont)



REFERENCE ARCHITECTURES EXAMPLE #2

# Agility without compromising on security

## Background

The business offers online gambling and is expanding at an exponential rate. IT must accelerate to keep up with demand while at the same time ensuring security of sensitive gaming and customer information. The business is constantly innovating to improve engagement with its customers and needs rapid application development. It must also make the best use of customer activity data to drive further engagement and profitability. The business needs access to best-in-class cloud capabilities for data analytics, development, research, etc.

The business has limited physical facilities, with a few small offices, but most employees work from home.

One of the key requirements for the business is ensuring a highly positive customer experience, but this must be done cost-effectively. IT, while generally scaling up as the business grows, must also be elastic enough to cater for variations in seasonal demand.

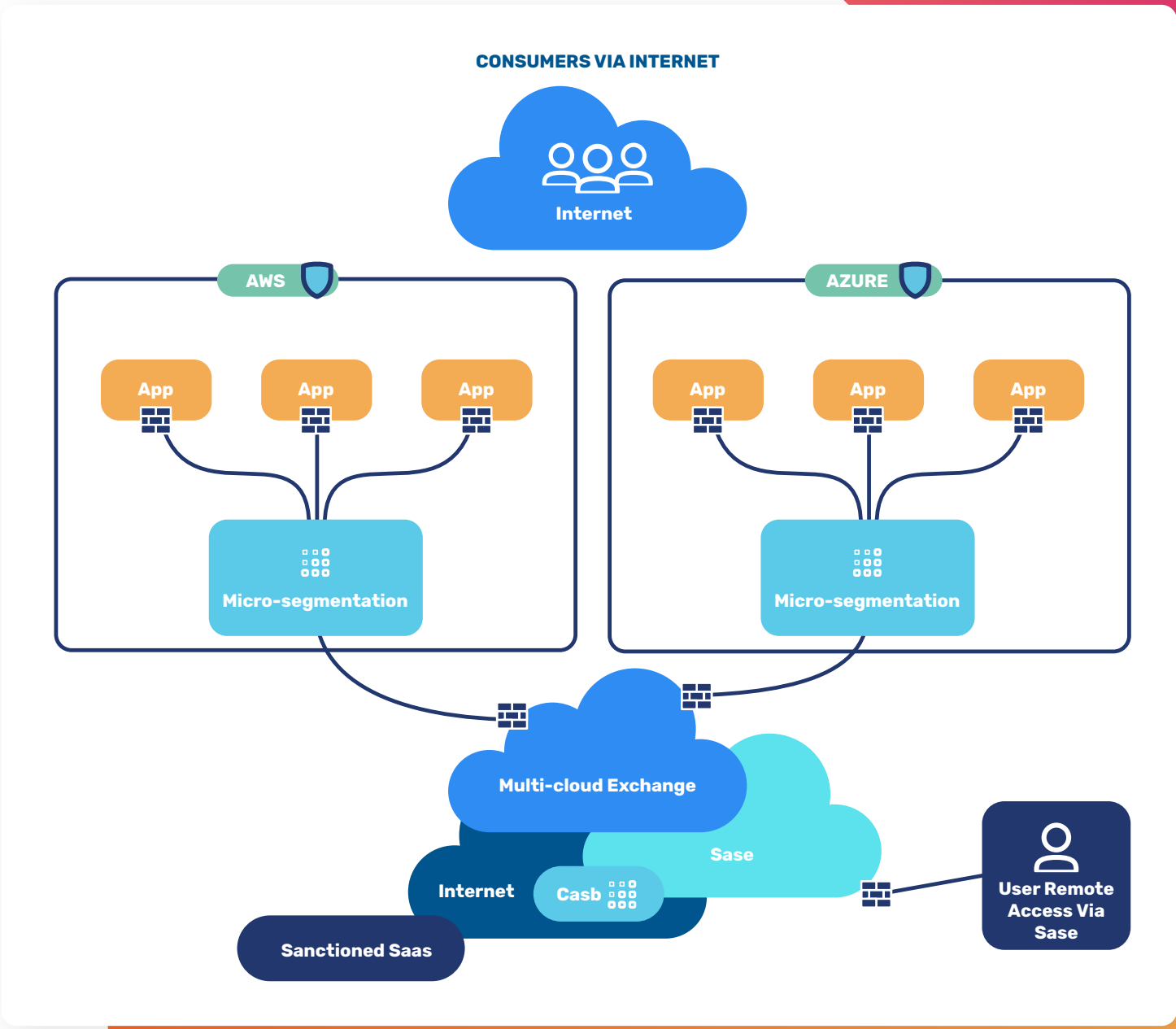
## Solution

The reference architecture will cover:

1. **Connectivity that will largely cater for work from home**
   a. Secure web gateways (SWG) and a software defined perimeter (SDP) is critical here
2. **Protection of user-facing applications (DDoS) and B2B interfaces (API/Bot protection)**
3. **Secure connectivity to cloud or multi-cloud**
   a. Multi-cloud or secure access to IaaS and SaaS is required
4. **A consistent application and view of security across the enterprise**
   a. Controls include agent-based micro-segmentation for cloud workloads
   b. This must account for the various atomic controls and offer a unified view and application of security
   c. Mobility must ensure that security remains attached to the workload
5. **User experience is important, and this must be managed**
6. **The network must be heavily automated as the busines is growing exponentially**
   a. This must address both security and good user experience
   b. Development pipelines need to easily and securely consume network constructs

REFERENCE ARCHITECTURES EXAMPLE #2

# Agility without compromising on security (cont)



# Conclusion

The process of working through a future state architecture exercise forces a business to think carefully about their plans and drives greater alignment between the business and IT. It provides a clear roadmap for network alterations and additions that ensure it is designed and engineered for a clear business purpose - and not just changed via a series of ad-hoc steps designed to solve the most pressing short-term problems.

Like any professional change process, it does take time, but that investment more than pays for itself with a network that is fit for purpose and addresses those three business problems we started with:

- **More secure**
- **Cost optimised**
- **Efficient and flexible**

TRUSTED PARTNERS

# Towards a Future State Architecture with Basis Networks

Working with large Australian businesses and enterprises, Basis Networks can help you bridge the gap between transformative business requirements and your future state architecture.

Through expert-led, ISO Certified consulting, integration and specialist support services, we solve the connectivity and security challenges brought about by both end-users and their organisation's growing reliance on devices and applications in a complex, hyper-connected world.

basis networks

1300 0 BASIS (1300 0 22747)
info@basisnetworks.com.au

basisnetworks.com.au