# ADAMnetworks Smart Rollout for a Zero Trust connectivity Network

## Smart Rollout Overview

A Zero Trust connectivity (ZTc™) network adheres to the Zero Trust best practice of deny by default and allow only verified known devices to connect to known good destinations. The goal of Smart Rollout is to go from the present state to a ZTc™ network with a predictable set of resources over a reasonable time period with little to no disruption to the business.

The table below outlines the general stages of a Smart Rollout of adam:ONE® with more details provided within each deployment model type. The estimated time can be anywhere from 1-8 weeks, depending on the size of the network and the amount of optimization required, particularly in stage 4.

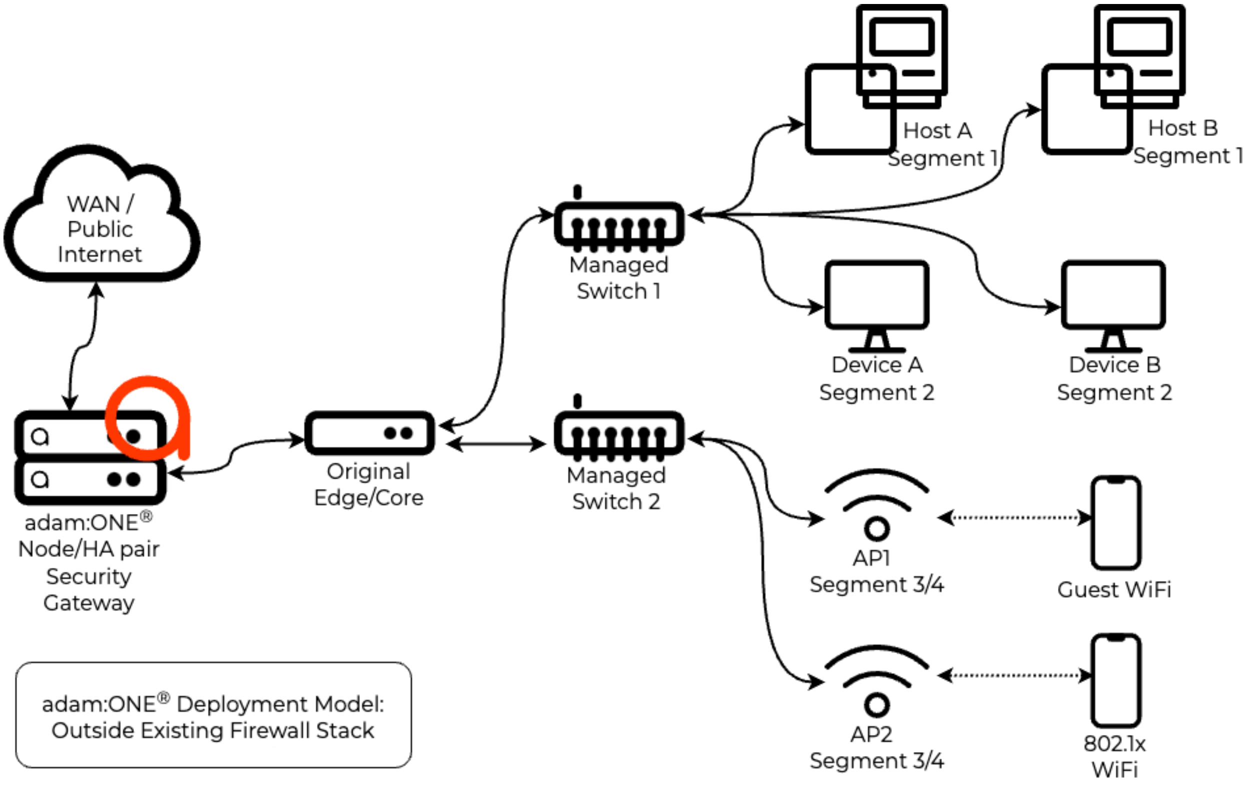
| Stage | Details |
|---|---|
| 1 - Consultation | Client Network map and outline including deployment model type |
| 2 - Preparation | Non-disruptive adam:ONE deployment and pre-staging in both cloud controller and on-prem include dashboard creation and utilizing pre-existing DNS server |
| 3 - Installation | This stage is designed to be preparatory and non-disruptive other than the brief re-cabling/re-routing change to insert pre-staged adam:ONE into the network with a small maintenance window. All endpoints should continue to function with the previous configuration of network protocols. |

| | |
|---|---|
| 4 - Network Tuning | In order for adam:ONE ZTc™ to function, this stage prepares any necessary network functions to facilitate the optimum environment for ZTc™. adam:ONE® to handle all DNS resolutions. Ensuring network segments that require cross communication are functional. This stage is done with test devices within each segment. |
| 5 - Device Identification | Non-disruptive stage where detailed observations are made in order to identify and take every discovered endpoint. Only applicable to deployments with layer 2 visibility requirements. |
| 6 - Policy shaping | Apply non-disruptive DNSharmony policies to network segments and Don't Talk To Strangers (DTTS®) for segments that require controlled DNSless based traffic. |
| 7 - Policy Hardening | Apply ZTc™ policies with DTTS® as default policy per network.  Stage works with Highest Value Assets (Servers), then Functional segments (VOIP, Printers, and other networking equipment), and finally End user devices |
| 8 - DNS Encryption | Apply DNS Encryption both internally and externally. This requires a maintenance window and adjustments to the adam:ONE® dashboard and a restart of the adam:ONE® muscle. |
| 9 - Integration | SIEM or other integrations are deployed for clients who have purchased these. |
| 10 - Maintenance Mode | adam:ONE® now goes into maintenance and monitoring mode |

# Deployment Models

Smart Rollout is applied to the following deployment models so that disruption to the business is limited or non-existent. These models allow the Enterprise to choose what type of configuration best fits their respective needs.

## Outside the edge of a network



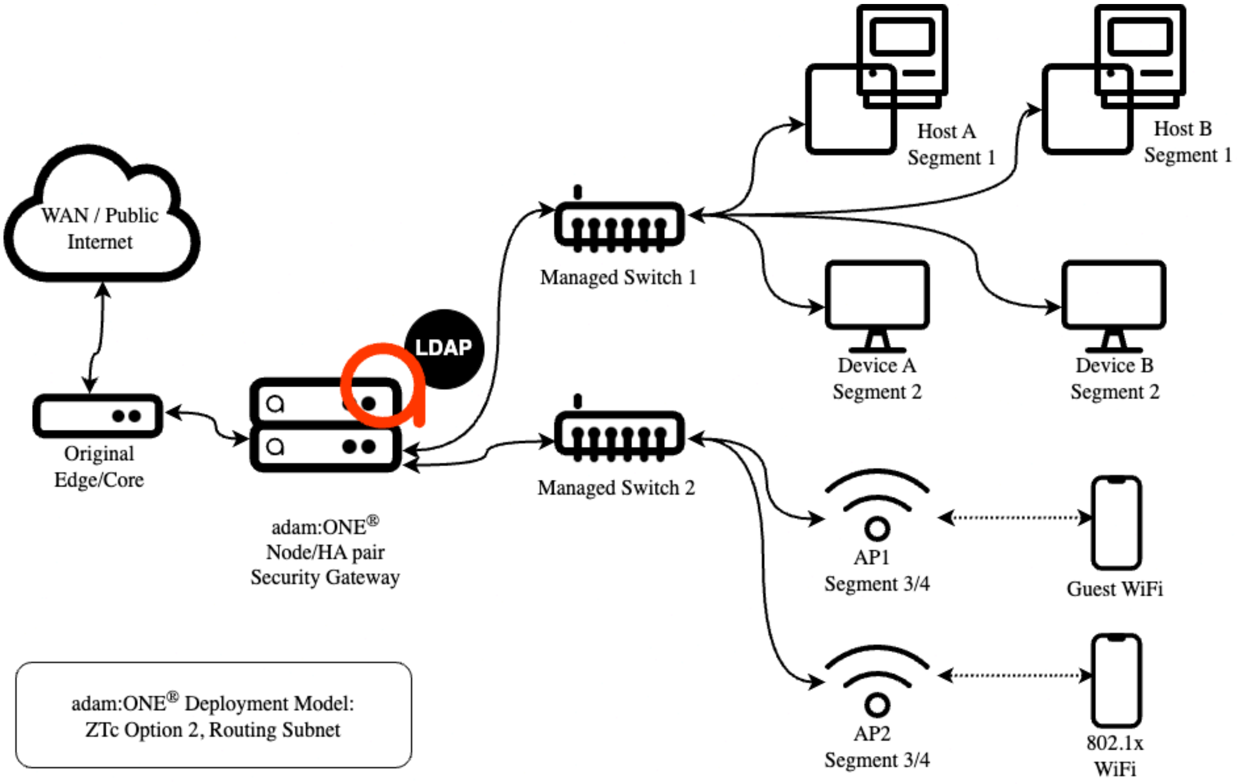
### Key deployment requirements:

- adam:ONE® requires 3 WAN IP addresses in the same subnet for High Availability (or single IP address for non-HA)
- Original Edge/Core WAN configuration and adam:ONE® LAN connection must introduce a net new private-class non-colliding 29-bit IPv4 subnet
- Per device policy only available if the Original Edge/Core is only doing pure routing

Outside the edge deployment requires no network or infrastructure changes other than the above listed one. Interoperability with existing systems is easily maintained. On a policy basis adam:ONE® will only see the downstream edge if NATing occurs within the Original Edge/Core which means no layer 2 visibility and no capability for per device policies or automated device inventory. However, a universal AdaptiveAI™, ReflexAI™ and DTTS® policy can be used to protect against Ransomware C2 connections and unauthorized connections to unknown domains or IP addresses from Phishing.

## Internal or Internal-bridged edge of a network

This has two deployment models a) as the internal edge or b) as the transparent internal edge or bridged mode.



### Key deployment requirements:

- adam:ONE® requires 3 LAN IP addresses in the same subnet for High Availability  or single IP address for non-HA
- For bridged infrastructure to support HA appropriate network engineering will be required
- Repeat for each internal segment
- Original Edge/Core WAN configuration and adam:ONE® LAN connection must introduce a net new private-class non-colliding 29-bit IPv4 subnet
- LDAP integration for device-tracking purposes allows for syncing IP to user/group

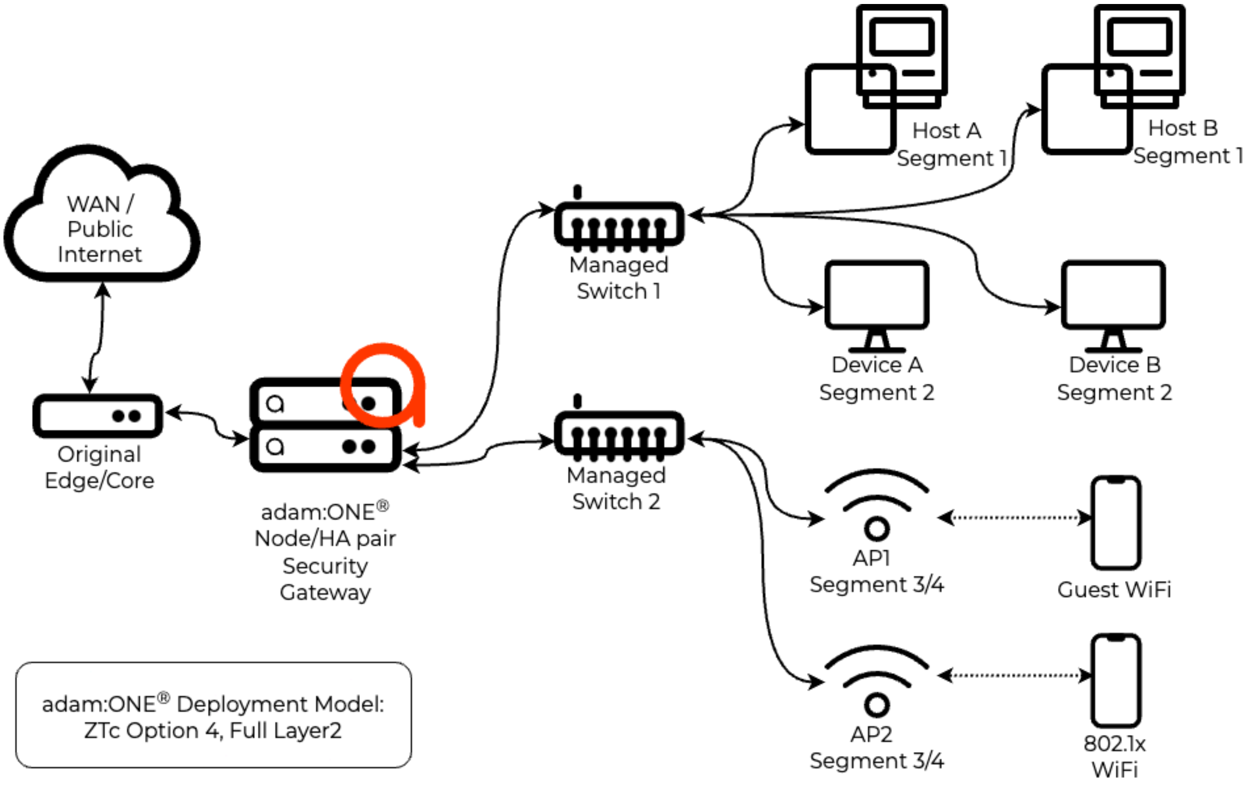
### As the Internal edge

Internal of the edge deployments require some additional changes to the configuration of adam:ONE® for each internal segment which needs protecting. This model provides access to all adam:ONE® features including full layer 2 visibility across the network which enables per-device policies, automated device inventory, and protection from shadow IT with a default “Holding Tank” policy for any new devices connected to the network. Compatibility with the current network stack will vary and may require some changes to the network configuration currently in use.

### As the Transparent Bridge

The transparent-bridged deployment has the placement of adam:ONE® in the same location as the Internal edge deployment. The advantage of this model is that no logical network changes are required. Layer 2 visibility can be accomplished with some L2 network redesign utilizing VLAN trunking otherwise per device policy can be done via IP addresses.

## Full Layer 2 of the network

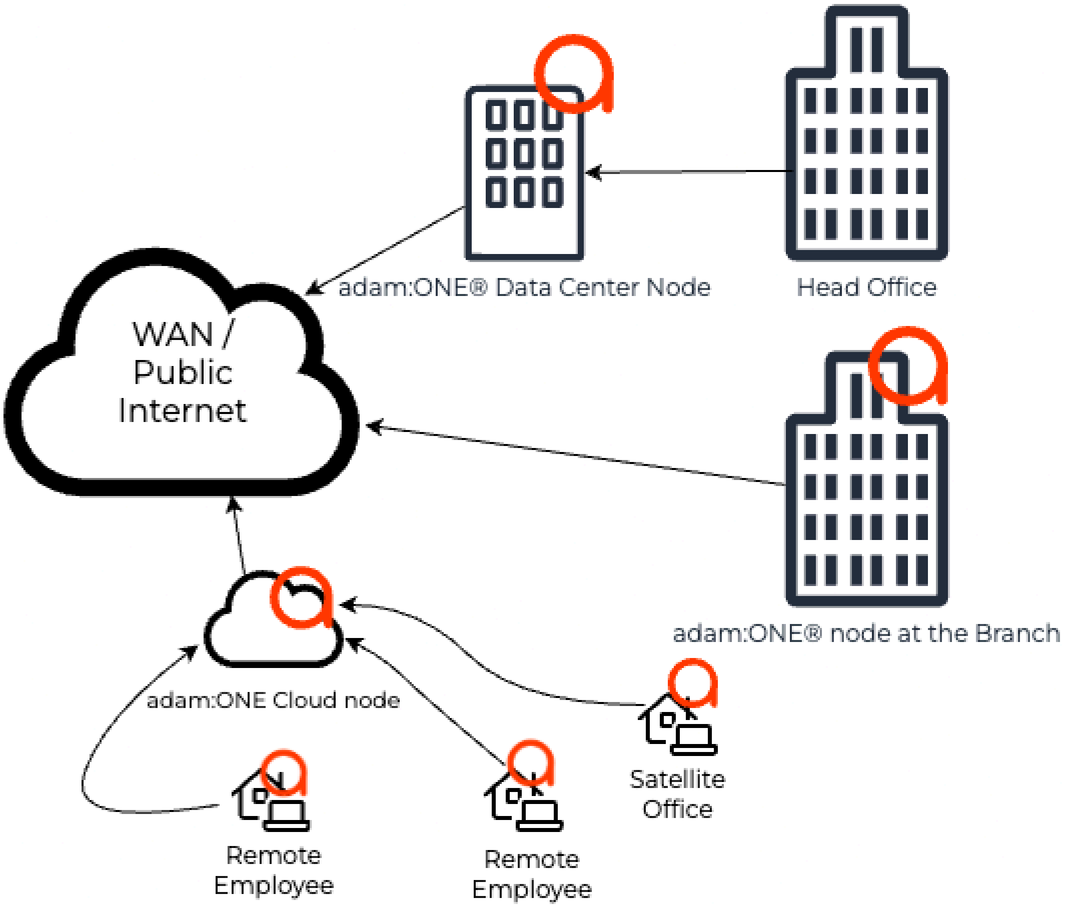


### Key deployment requirements:

- adam:ONE® requires 3 WAN IP addresses in the same subnet for High Availability (or single IP address for non-HA)
- 3 internal IP addresses for each LAN segment

The Full Layer 2 deployment model requires network infrastructure changes and additional configuration but provides access to all adam:ONE® features. Full layer 2 visibility, automated device inventory, shadow IT protection, per device policies, micro-segmentation, and default “Holding Tank” policy.

## Multi-Site Deployment



adam:ONE™ can be deployed across multiple sites according to the needs of the Enterprise. At the Data Center level for aggregated traffic, site specific locations and cloud deployments. Each of the various deployment models can be utilized either physically or virtually.

## Smart Rollout Summary

Smart Rollout provides a predictable, low to none disruption experience for clients to transition from a traditional network which fails open to unknown domain and IP connections into a Zero Trust connectivity (ZTc™) network where the Enterprise has full connection control. A ZTc™ network goes from trying "block the bad" to "allow only the known and verified" without disrupting the business.

**ADAMnetworks - Protecting the people and systems you care about.™**