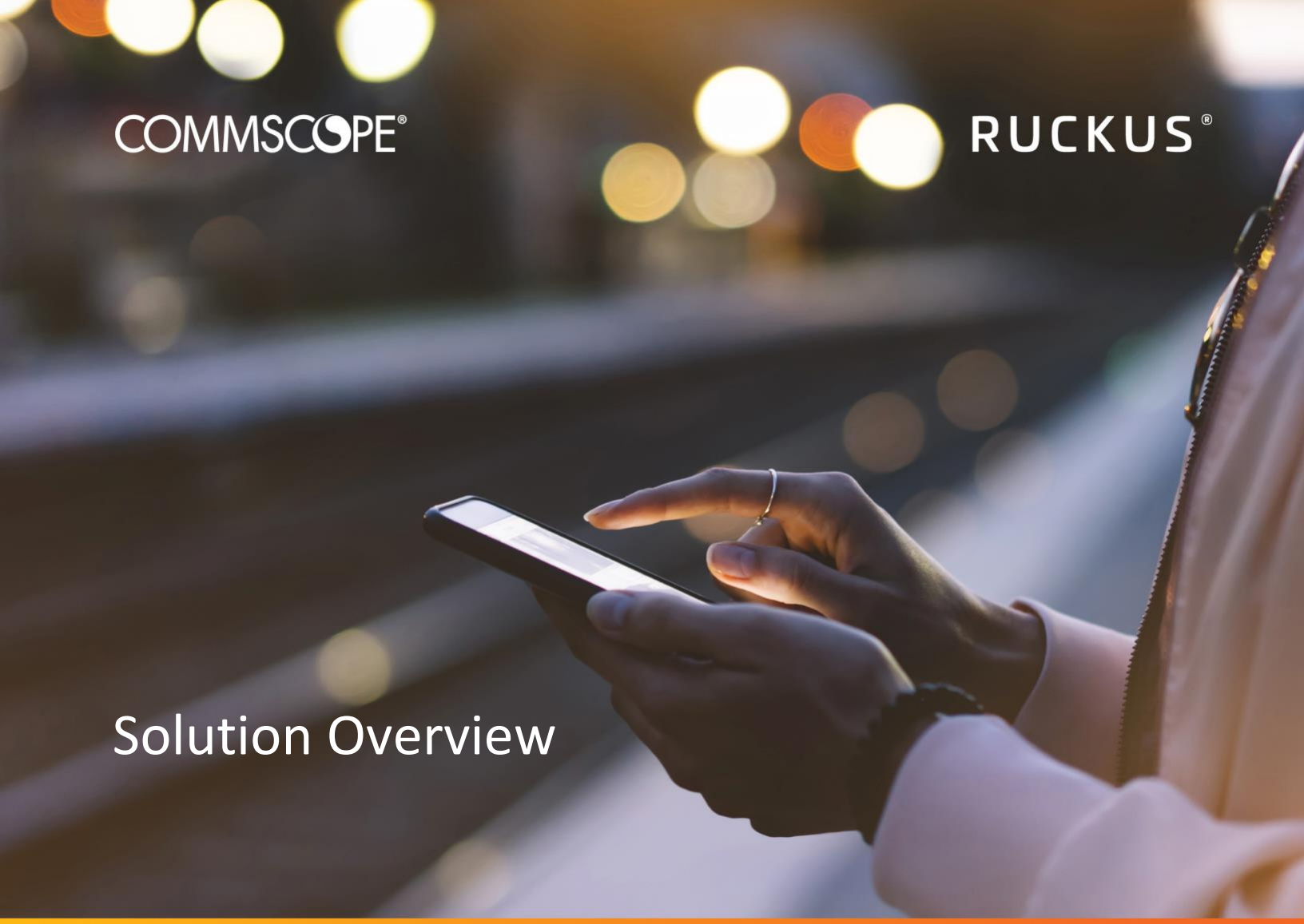

COMMSCOPE®

RUCKUS®

Solution Overview

RUCKUS & Infiot SD-WAN Solution Overview

January 2022

Table of Contents

Overview

This document presents an overview on SD-WAN solutions using RUCKUS access points, ICX switches, Cloudpath and Infiot products. It covers use cases and benefits, the main components and the technologies involved.

Who is Infiot?

Named a Cool Vendor by Gartner in 2021, Infiot is a pioneer in enabling secure, reliable access for all remote user devices (smartphones, laptops, IoT), sites and cloud.

Infiot is based in San Jose, CA. It was founded in 2018 and it is funded by Lightspeed Venture Partners, Neotribe Ventures, and Westwave Capital.

Infiot goes beyond SD-WAN, enabling the creation of borderless enterprise networks which include zero trust security, network optimization, edge-intelligence, and AI-driven operations (ZETO – Zero Trust and Optimization)

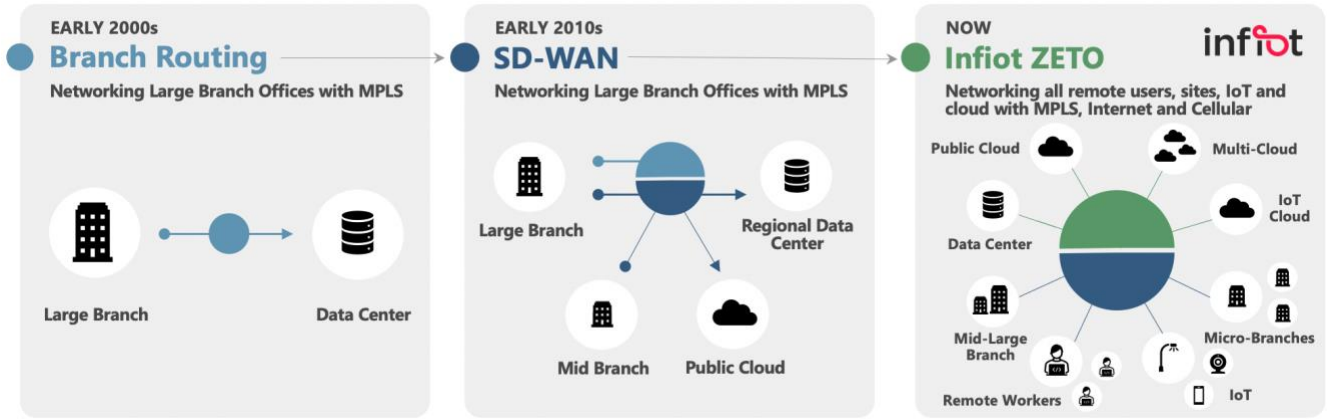

FIGURE 1 - SD-WAN EVOLUTION

ZETO Architecture

The rise of cloud services, the emergence of IoT and Work from Home (WFH) are expanding the enterprise networks beyond corporate offices. That will require a modern approach to quickly configuring, connecting, and securing devices and applications at the edge of the cloud network, wherever they may reside.

Future work patterns will require that every employee, every site, and every device should be considered as extended branches of the organization. This involves the ability to extend the enterprise WAN using the same policy - with speed, application assurance, and security in mind - whether it is a home office or an office, an ad-hoc POS, or an employee on the go.

These new connected digital workspaces are an extension of the organization and part of the emerging Borderless Enterprise.

Infiot has built a unique ZETO (Zero Trust and Optimization) architecture to address the borderless enterprise use cases. ZETO is fully compliant with SASE (Secure Access Service Edge).

The ZETO architecture has three main components:

- ZETO Edge
- Cloud Orchestrator
- Cloud Controllers

ZETO Underlay/Overlay Architecture

Infiot ZETO Edge includes hardware options, a virtual hub, and a Windows 10 Pro client (a future client release will support macOS)

The Infiot Orchestrator is a multi-tenant cloud portal to configure sites, virtual hubs, edges, and policies, as well as to monitor all connections, users, and applications.

The Infiot Controller also run in the cloud, to manage the control plane of the SDN network.

The underlay is the IP network provided by the enterprise or service provider. The routing tables to reach the endpoints are established using public IP addresses, NAT, static routes or BGP. In larger deployments, such as in Data Centers with High Availability topologies, the Infiot Edge devices and hubs are configured with BGP. In small deployments, like remote offices or Work from Home (WFH) use cases, the edge devices can simply use a default or static route to reach the other end of the VPN.

The overlay network uses IPSec VPN tunnels. The tunnel endpoints are the Infiot Edge devices and virtual hubs. The users' traffic towards the corporate DC runs on a trusted network across the VPN tunnels. The edge devices also support local breakout for Internet traffic and access to cloud services, without the need to go across the corporate DC.

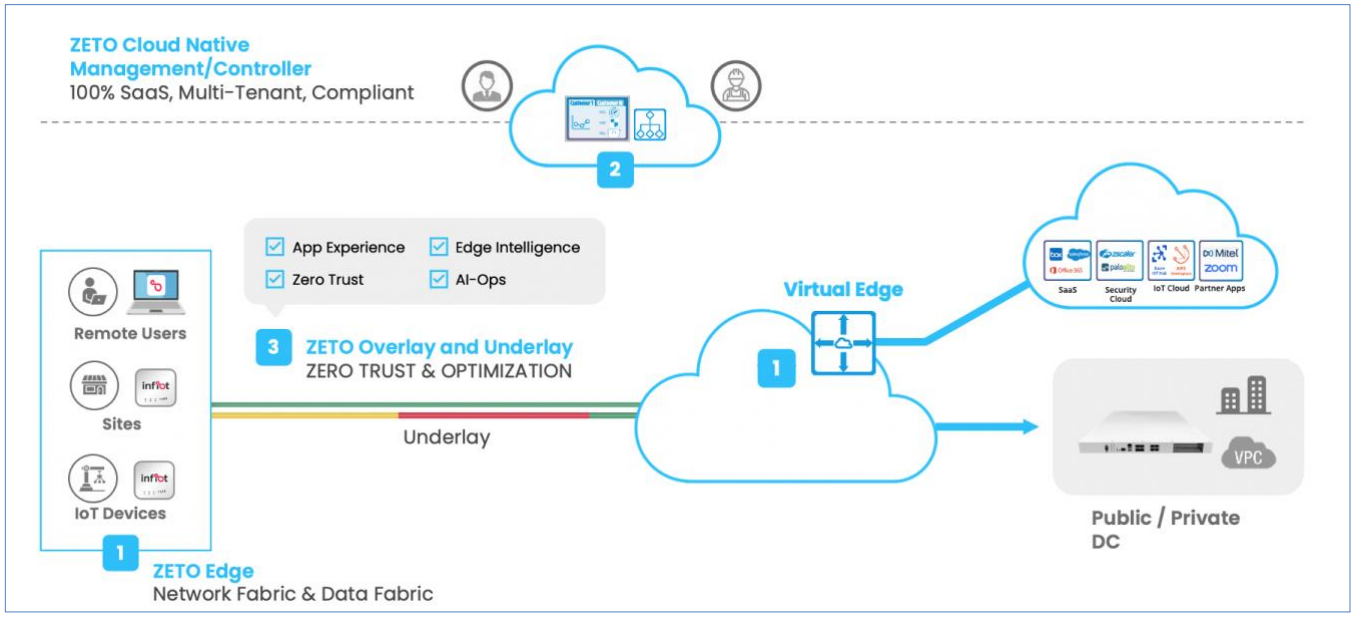

FIGURE 2 - ZETO UNDERLAY/OVERLAY ARCHITECTURE

ZETO Edge Deployment Options

There are several options to deploy ZETO Edge:

- **Hardware appliances** - routers scaling from 100 Mbps to 5 Gbps of encrypted traffic, with ethernet LAN and WAN interfaces
- **Cellular Gateway** - a router model including ethernet and LTE WAN interfaces
- **ZETO Client -** Windows 10 Pro/Windows 11 client software (macOS is planned)
- **Clientless Access** - a method to access a remote workstation remotely, without any client software
- **Cloud Services Fabric** - virtual edge software, scalable up to 2 Gbps of encrypted traffic, to be deployed as ESXi VMs

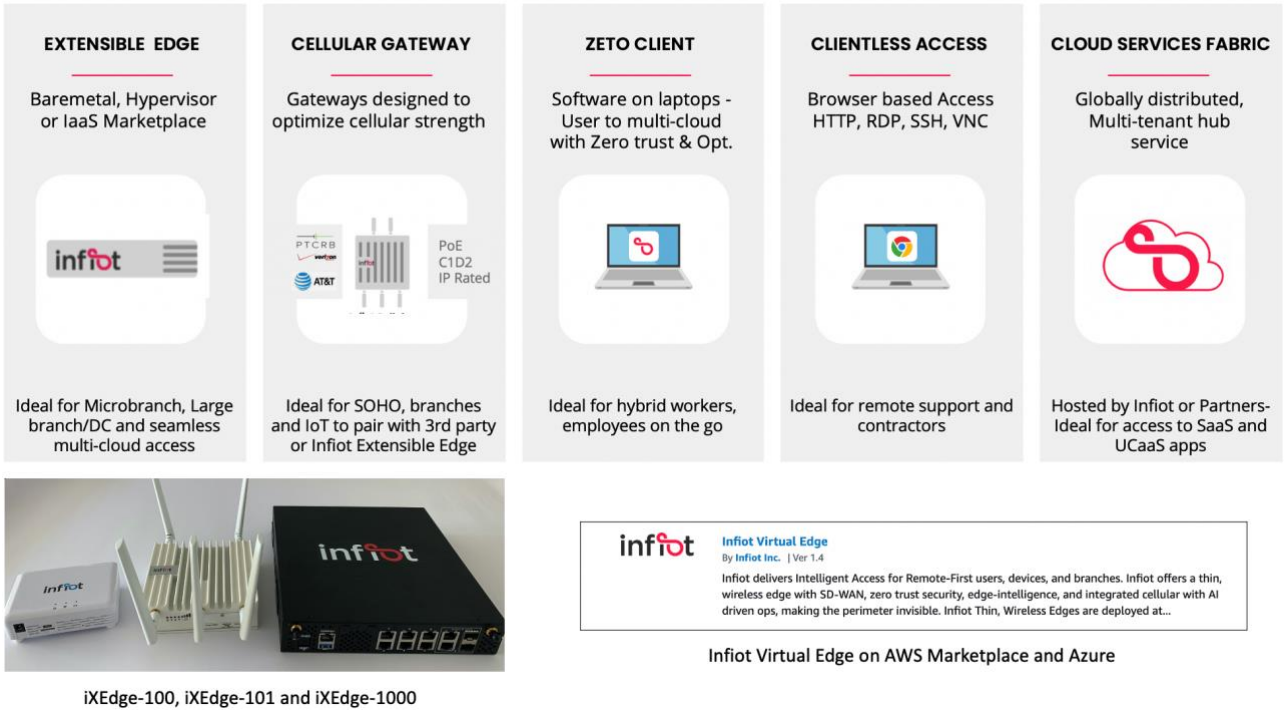

FIGURE 3: ZETO EDGE DEPLOYMENT OPTIONS

ZETO Edge Hardware Device Quick Specs

	IXEDGE-100	IXEDGE-101	IXEDGE-1000	IXEDGE-3000 (roadmap)	Virtual Edge
Throughput (encrypted)	100 Mbps	100 Mbps	1 Gbps	5 Gbps	1 Gbps (2 cores) 2 Gbps (4 cores)
LAN/WAN (1G RJ45)	3	4	6	6	Up to 8 virtual interfaces
LAN/WAN (10G SFP+)	N/A	N/A	2	2	----------
Integrated Wi-Fi	2.4 GHz/5 GHz 802.11ac 2x2 MIMO	2.4 GHz/5 GHz 802.11ac 2x2 MIMO	2.4 GHz/5 GHz 802.11ac 2x2 MIMO	N/A	----------
LTE	USB	Integrated/USB	USB	N/A	----------

TABLE 1: HARDWARE DEVICE QUICK SPECS

Infiot Cloud Orchestrator and Controller

The Infiot Cloud Orchestrator and Controller offer the following features and benefits:

- **One-click Service Marketplace** - Ensures rapid deployment of Infiot or partner services closer to users, devices or in the cloud.
- **100% SaaS Controllers** - Achieve resilience by separating control plane and data plane and deliver operational simplicity and scale with industry's first 100% SaaS based cloud-native controllers.
- **AI-Driven Operations** - Achieve operational simplicity with automated troubleshooting and AI-Driven insights. Self-healing with Infiot's unique dynamic policy enforcement to reduce the number of support tickets.
- **Proactive AI-Driven support** - Flow analytics, anomaly detection and secure inbound access deliver proactive support and helps maintain end user service level experience with short time to resolution.
- **Security Compliance** - PCI Level 1 and HIPAA certified cloud-hosted service that are distributed in Tier-1 data centers, certified with SAS70 Type II, SSAE16, and ISO 27001.

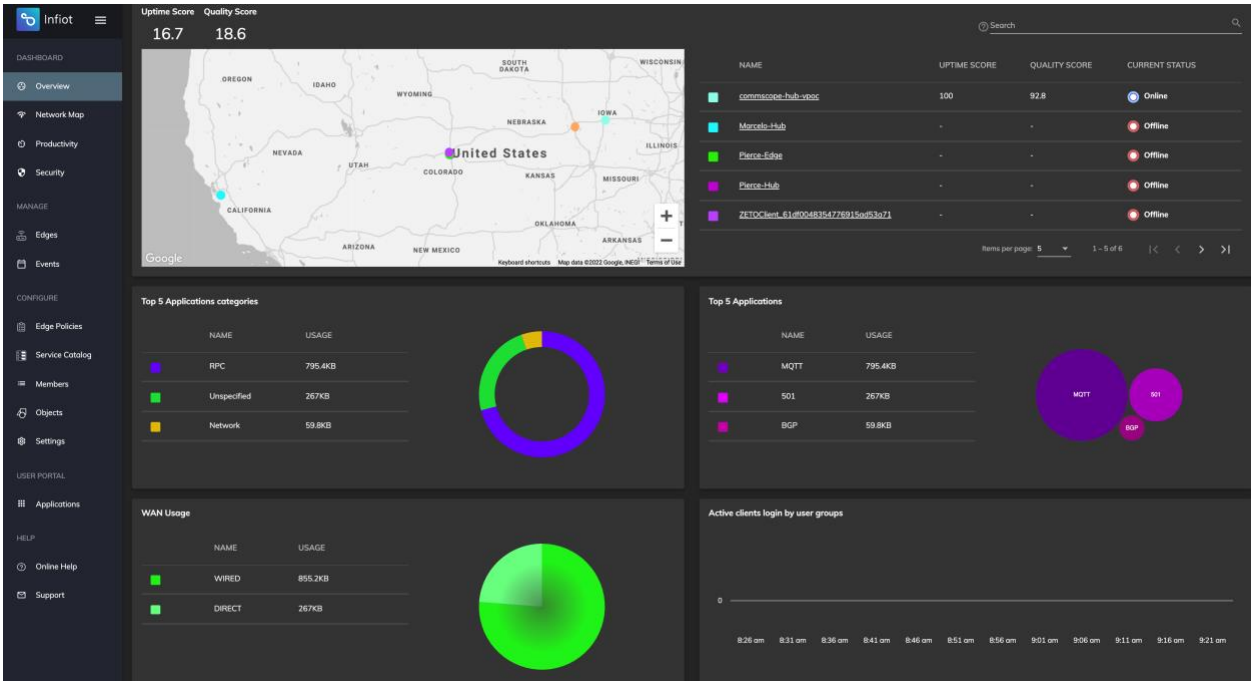

FIGURE 4: INFIOT PORTAL DASHBOARD

Use Cases

Many different use cases are supported using Infiot and RUCKUS. Some of the use cases include:

- **Hub & Spoke** - This is the most basic topology, used for remote workers and work from home, where an iXEdge device in the remote office or home establishes a VPN to a Virtual Edge in the enterprise network. Policies configured on the edge device define which resources can be accessed by the remote workers.
- **Proxy ARP** - The iXEdge is configured with Proxy ARP, forcing all traffic among the workstations to pass though the iXEdge. That way, the QoS policies configured on iXEdge will also be enforced for the workstations traffic, without changing the network topology.
- **Dual-Homed DC** - This is a use case where a high-capacity DC has connections to multiple ISPs and has two Virtual Edges dual-homed to the internal routers. The inbound and outbound traffic rules are defined by BGP policies configured in the Virtual Edges and internal routers.
- **Firewall Policies** - Every use case can be configured with firewall policies. In the example shown at Figure 5, firewall rules determine that only the Point-of-Sales input devices can access the POS server in the datacenter.
- **Spoke with LTE backup** - iXEdge-101 has integrated LTE, and iXEdge-100 and iXEdge-1000 supports LTE using an USB dongle. The LTE interface can be used as a backup when the wired WAN interface is down.
- **Spoke High-Availability using VRRP** - Two iXEdge devices can be connected using the OPT port, using VRRP for high-availability.

The following diagram shows the topologies for all use cases:

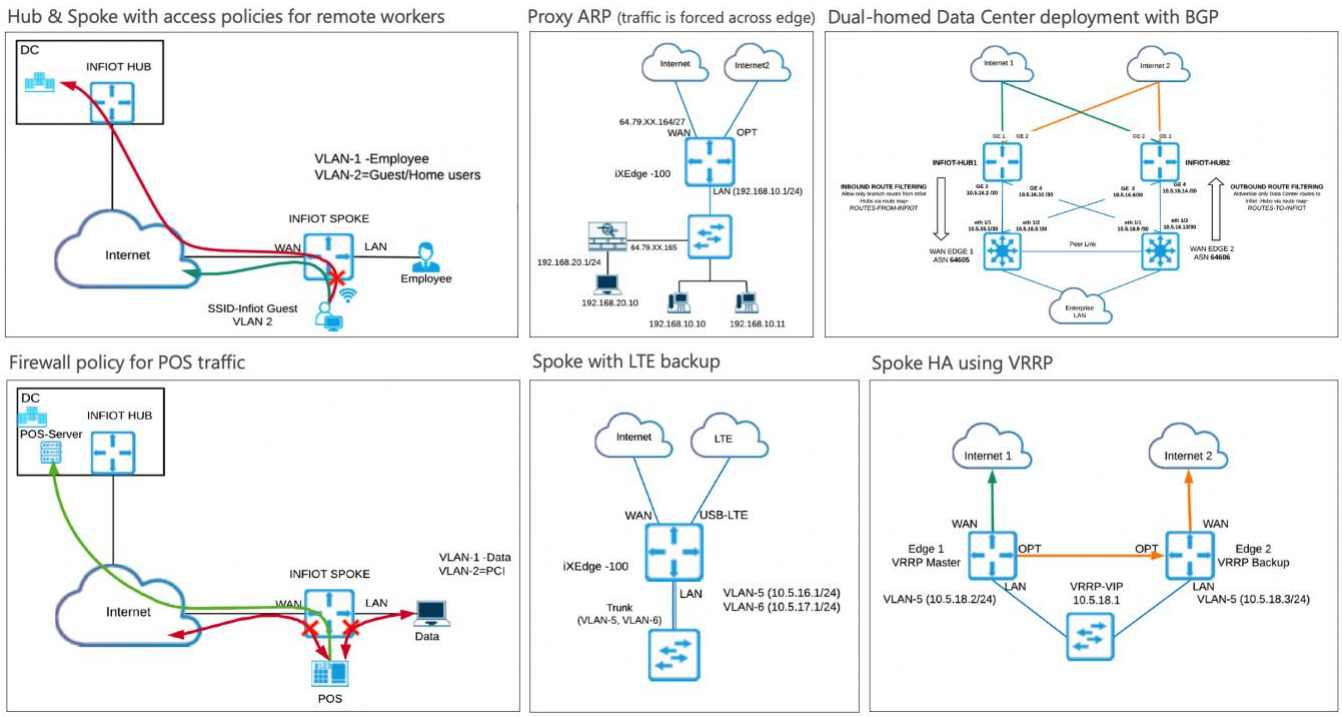

FIGURE 5: USE CASES

Infiot ZETO Capabilities

All Infiot devices and the ZETO client run the same Infiot software, and offer the same capabilities:

Zero Trust Security

Infiot software follows the SASE paradigm. Infiot delivers unparalleled security with a converged zero trust architecture that protects you from threats and keeps you compliant anywhere - consistent security across clients on laptops, thin wireless edges, or browser-based security.

Instead of trusting an IP address, Zero Trust verifies the identity of the user and device using an identity provider (IDP) such as Okta or Azure AD. Access policies based on user identity and device posture are applied to the user traffic, no matter the connection type, wired or wireless.

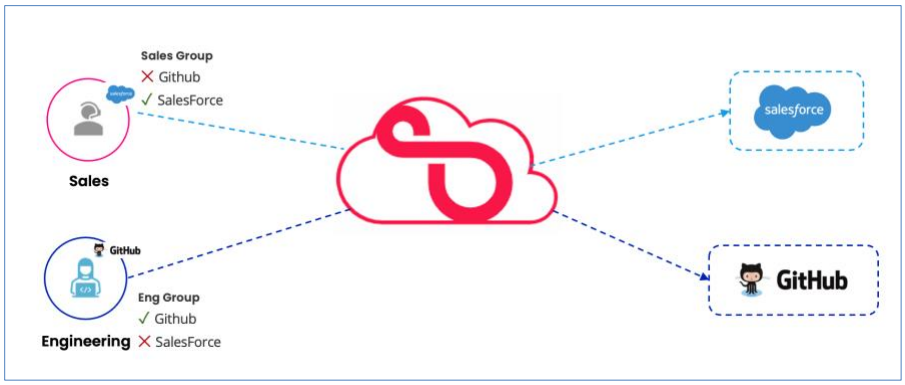

FIGURE 6: ZERO TRUST SECURITY

Edge Intelligence

Simple click-to-enable services can be seamlessly deployed at the edge or in the cloud. The container-based edge eliminates the need of multiple single function branch appliances, with the ability to instantiate and run additional services such as application performance monitoring, firewall, IDS/IPS, and third-party services inside the iXEdge. Examples include Thousand Eyes, SpeedTest and Azure IoT Edge.

FIGURE 7: EDGE INTELLIGENCE

AI-Driven Operations and Assured Application Experience

Infiot monitors **User Service Level Experience** data - per user and per minute, helping to reduce time to resolution for bad user experience, with insights into the Service Provider SLAs or policies, from the client to the destination. Infiot's control plane software includes automatic remediation and self-healing using dynamic policy enforcement and dynamic path selection to reduce trouble tickets.

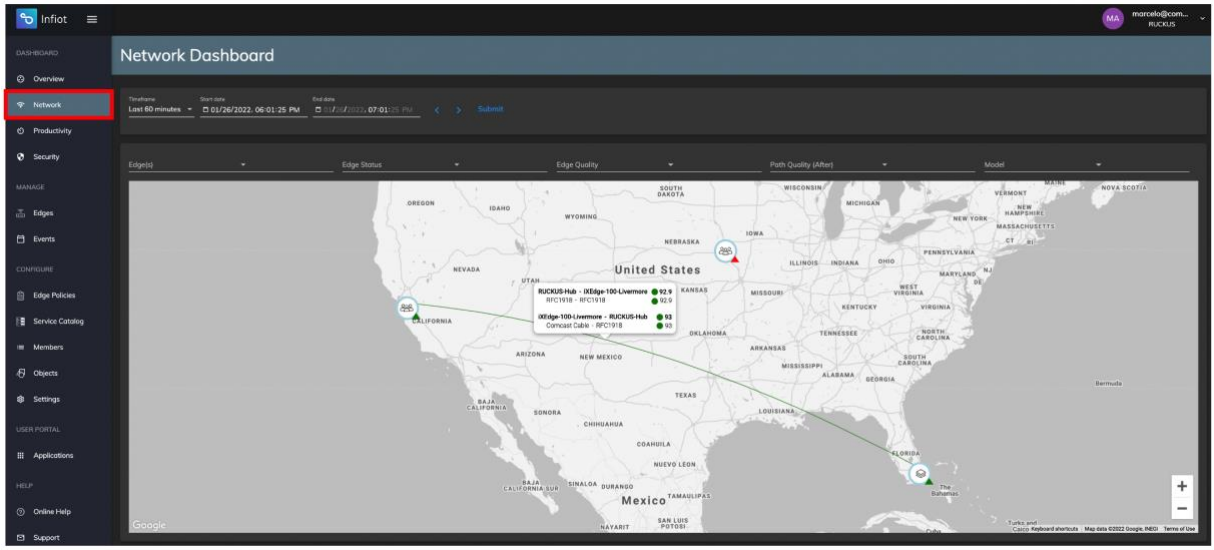

FIGURE 8: SLA MONITORING

You can monitor the user traffic end-to-end, with full visibility of the path from the user device to the application. Infiot Edge includes a DPI engine to detect applications and URLs, and it offers dynamic path selection with sub-second blackout/brownout protection

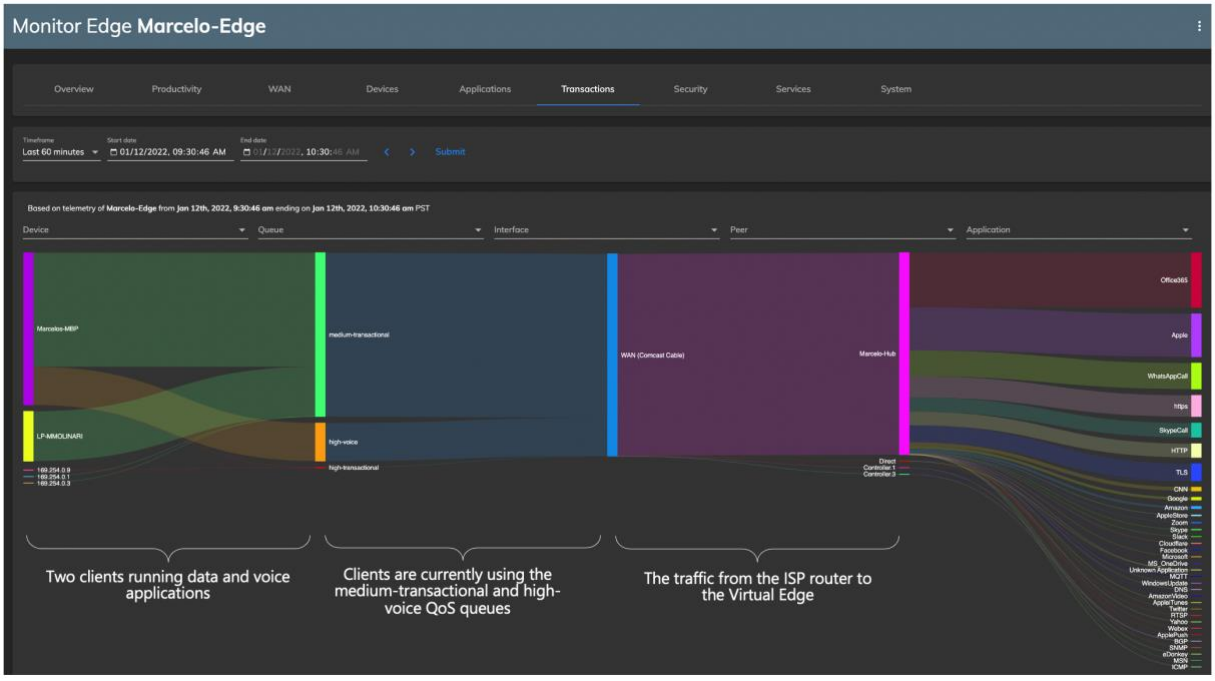

FIGURE 9: APPLICATION MONITORING

RUCKUS & Infiot Reference Architecture - Work from Home (WFH)

The RUCKUS & Infiot Reference Architecture for Work from Home uses an Infiot Edge device in line with a RUCKUS ICX switch. The Infiot Edge device has Wi-Fi disabled. RUCKUS access points connected to the ICX switch provide will provide wireless access. The RUCKUS access point can be of any model, managed by RUCKUS Cloud, SmartZone or Unleashed.

In the diagram below we are using an iXEdge-100 in the home office. It supports up to 100 Mbps of IPsec traffic or up to 200 Mbps of unencrypted traffic. The iXEdge devices are routers. Its WAN and LAN interfaces need to be in different IP subnets. Normally, it will receive the IP address for its WAN port from the ISP home routers, and it will provide IP address for the devices downstream (the ICX switch, RUCKUS access points and wired/wireless clients) using its own DHCP server.

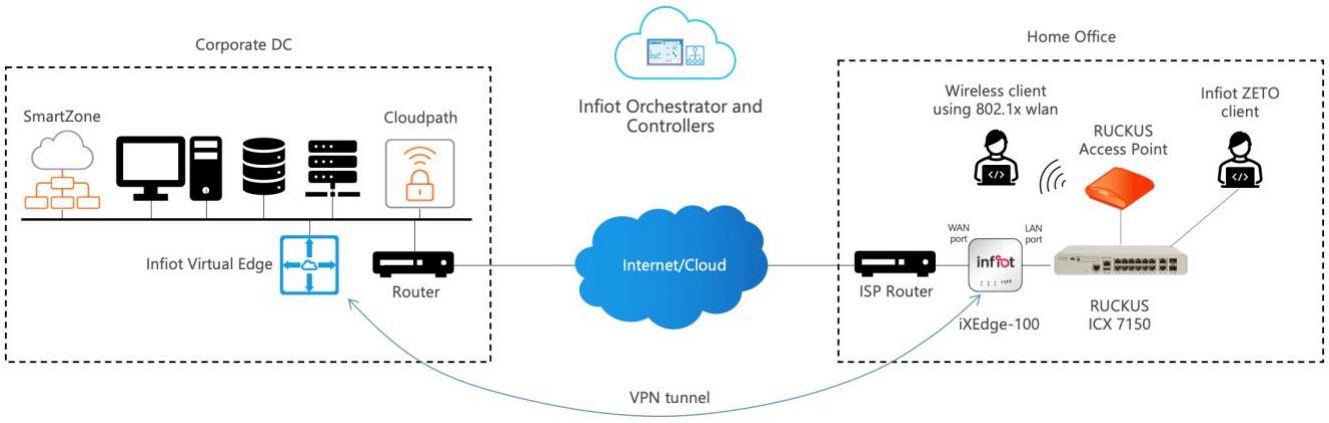

FIGURE 10: RUCKUS & INFIOT REFERENCE ARCHITECTURE - WFH

The iXEdge-100 establishes an IPsec VPN tunnel to the Virtual Edge, which supports up to 1 Gbps of traffic with 2 cores, and up to 2 Gbps with 4 cores. By default, no traffic is allowed across the tunnel. An edge policy or firewall rules need to be configured to allow access to corporate resources.

A fully compliant SASE solution requires user identification by an Identity Provider (IDP). Cloudpath's RADIUS can be used as the IDP. The RADIUS attributes in the authentication response can be used to assign group policies to the wired or wireless clients. A wireless client will connect to an 802.1x WLAN configured in the RUCKUS access point, and the wired client can use the Infiot ZETO client. It is also possible to configure traffic policies in the iXEdge-100 only, without using 802.1x or and IDP. Although supported, that will not be a fully compliant SASE solution.

The iXEdge-100 also supports local break-out (LBO), so the users can access the Internet or cloud services directly, without having to pass through the Corporate DC. Firewall and URL policies can also control the user access.

References

Infiot

- Infiot web site
  https://www.infiot.com

Other RUCKUS collaterals

- Design Guide – RUCKUS & Infiot WFH Design Guide
- Design Guide – Cloudpath & Infiot Integration Guide
- Design Guide– Infiot ZETO Client Configuration

Ruckus solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit **commscope.com** to learn more about:

- Ruckus Wi-Fi Access Points
- Ruckus ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT

COMMSCOPE®

RUCKUS®

commscope.com

Visit our website or contact your local CommScope representative for more information.