SOLUTION OVERVIEW

RUCKUS Networks Zero Trust Architecture (ZTA)

Why is Zero Trust so important?

Zero Trust Architecture (ZTA) is critically important for modern network security due to the escalating threats posed by sophisticated cyberattacks. Its fundamental principle, "never trust, always verify," has grown increasingly relevant as it shifts the focus from merely securing network perimeters to securing individual access requests and transactions, irrespective of location. This approach emphasizes the idea that any endpoint or user could potentially be compromised, and therefore, every interaction should be authenticated, authorized, and encrypted. In doing so, it minimizes the risk of unauthorized data access, protects sensitive information, and mitigates potential damage from breaches, thereby enhancing the overall security posture of organizations in a digital era marked by remote work, cloud services, and an ever-expanding attack surface.

The Challenge

Securing your network, and the information contained within that network, isn't a matter of just implementing a tool and moving forward. First, it has to be part of your way of thinking – you have to accept that your network must verify everything, that bad actors may get inside and it is your job to detect and stop them, and that there are multiple ways to enforce policy, protect against intrusion, expand visibility to manage and control your network, and minimize access even if a penetration occurs. In essence, security has to be designed into your network, built upon policies, procedures, and controls, and implemented consistently and repeatedly to make sure that connections to network elements, devices, software tools, environments, and applications are validated. It also involves making sure that too much access isn't given to any one user or role, known as "least privilege". Given the lifecycle of devices, security capabilities of different elements connected the network, the myriad of users and devices from guest access and corporate users of BYOD devices to company-issued and controlled devices, securing your network can be seen as a very complex undertaking.

Elements of a ZTA Solution

ZTA has a number of essential requirements. Generally, a Zero Trust Architecture includes the following elements:

- ***Identify Verification****:* every user's identity must be verified before they are granted access, regardless of their location or the network they're using.
- ***Microsegmentation***: This involves breaking down security perimeters into small zones to maintain separate access for separate parts of the network. If a breach occurs, microsegmentation helps contain it and prevents it from spreading across the network.
- ***Least Privilege Access***: Users should only have access to the resources they need to perform their tasks, and nothing more. This minimizes each user's attack surface and reduces risk.
- ***Multi-Factor Authentication***: MFA verifies a user's identity by requiring multiple pieces of evidence, or factors, before granting access.
- ***Network Visibility****:* Complete visibility into the network is crucial in Zero Trust. This involves understanding who the users are, what devices are being used, the nature of the data in the network, and the context of user access.

RUCKUS® COMMSCOPE

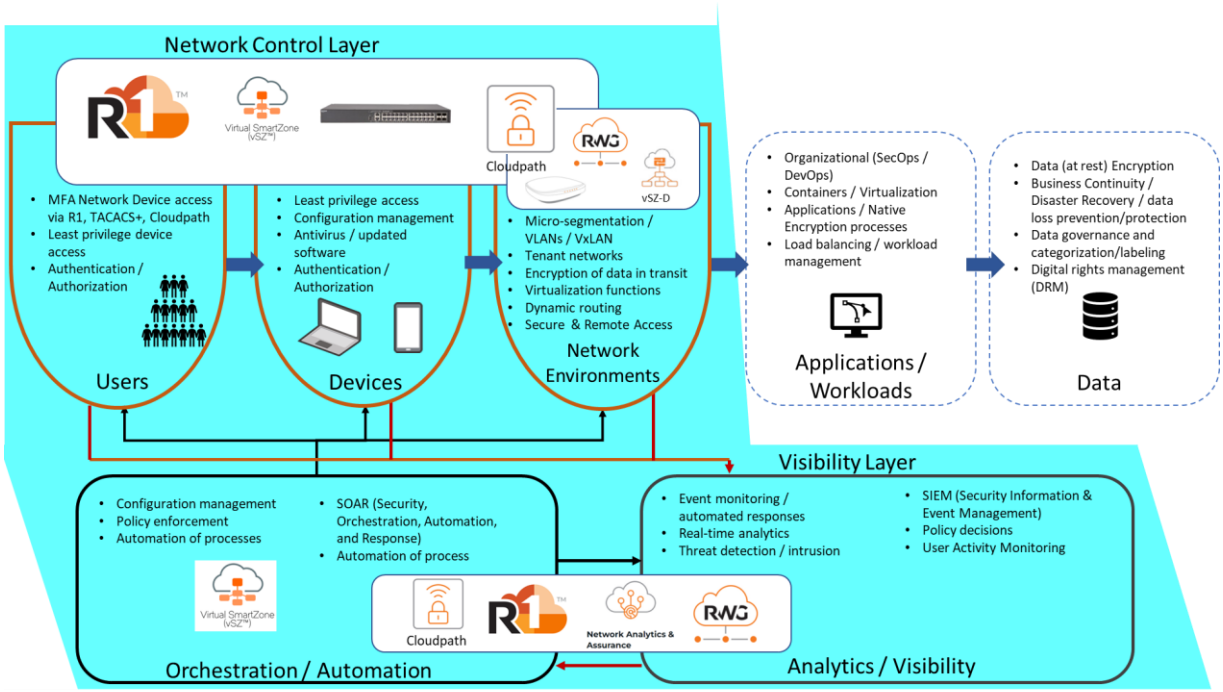
- ***Real-time Analytics and Automated Responses**:* ZTA should include AI and machine learning technologies to analyze network behavior in real time, detect anomalies, and automate responses to suspicious activities.
- ***Secure and Remote access**:* Implementing a secure remote access solution, such as a Virtual Private Network (VPN), to facilitate secure connectivity for remote users, is a first step towards securing a network, but is often augmented with more robust Zero Trust capabilities to avoid bottlenecks and scaling issues.
- ***Encryption**:* All data, both at rest and in transit, should be encrypted.
- ***Policy Enforcement**:* Policies that dictate user access and permissions should be enforced uniformly across the network.
- ***Security Orchestration, Automation, and Response (SOAR)**:* ZTA should include SOAR technologies to automate threat detection and response, improve efficiency, and mitigate risks.

RUCKUS ZTA Solution

By implementing a Zero Trust Architecture leveraging RUCKUS Networks' extensive portfolio and selected third party solutions, organizations can enhance their security posture and protect against potential threats. It is the nature of network security that Zero Trust can't just be at one layer but must involve multiple levels of security. Therefore, a robust Zero Trust solution must have all network and associated devices -- wireless products, wired products, software-enabled features and capabilities, the RUCKUS® WAN Gateway, and proven partner solutions, products and integrations – configured and acting according to Zero Trust principles.

The RUCKUS approach to ZTA involves bringing together devices and software to address the necessary components for a Zero Trust model. Based upon the security risk posture, complexity of the business and environment, and organization's ability to support dedicated network security operations, certain elements within a Zero Trust Solution will change.

Since RUCKUS products are designed to work seamlessly with existing network infrastructures that use industry standard protocols, RUCKUS solutions can be implemented alongside existing ZTA components while choosing the appropriate RUCKUS solutions to complement those components. By using a multivendor approach, one can benefit from the flexibility and innovation of different vendors to build out the Zero Trust Architecture and leverage the support and expertise of multiple partners.



RUCKUS Networks Zero Trust Architecture is within the boundaries of managing the network from edge inwards

Identity Verification

RUCKUS enables you to validate identity and manage access. To do this, RUCKUS recommends that you use one of RUCKUS's flagship tools and couple that with configuration best practices.

- Deploy RUCKUS Cloudpath® Enrollment System for network access, authentication, and authorization, with the latest encryption (WPA2™/WPA3™), dynamic pre-shared keys (Dynamic PSK™), and certificates to cut down on administrative overhead and accelerate onboarding while providing improved security over traditional wireless network access methods.
- Utilize Cloudpath solution to provide centralized user authentication, authorization, and accounting.
- Integrate RUCKUS SmartZone™ controllers or RUCKUS One™ with a Cloudpath solution to enforce user identity verification and access control.

- Enable AAA/RADIUS authentication integrated with Cloudpath solution, RUCKUS One, or RUCKUS SmartZone to help ensure only authenticated and authorized users can access the network.
- Check continuously that access is authorized by implementing the RUCKUS WAN Gateway (RWG) for network access control (NAC) for persistent posture checking to make sure BYOD and corporate devices are up-to-date and secure.
- Implement RWG's or similar provider's firewall to only allow devices in that have passed security validations.
- For multi-tenant situations, such as in shared living space in multi-dwelling units, utilize Cloudpath solution's unique solution, utilizing Dynamic PSK technology so that each resident can see and manage only their own devices on their network.

Microsegmentation

To limit the exposure within your network, it is a best practice to also segment your network into smaller zones. Each zone is assigned access and that is limited to what each zone within the network is allowed to see and do. "zones" are really VLANs or VxLANs that are implemented at the wired switch architecture and carried through to the wireless access points, which then allow devices to log in and be assigned to VLANs/VxLANs based upon their roles and credentials. Implementing microsegmentation can be done in various ways, but a typical configuration would do the following:

- Leverage RUCKUS ICX® switches to enforce VLAN or VxLAN policies and control traffic flow between segments. Depending upon your overall wired architecture, you would choose either VLANs or VxLANs to implement segmentation at the switch level, which then carries to the rest of the network.
- Use VLANs/VxLANs to divide the network into smaller, isolated segments based on logical or physical boundaries, isolating guest networks, and device traffic; fundamentally, this addresses your "North-South" traffic into/out of the different networks defined by your VLANs.
- Utilize RUCKUS wireless access points (APs) with built-in VLAN support to extend the VLAN/VxLAN configuration allowing separation of traffic between different user groups, devices, or applications.
- Implement the RWG to create "East-West" traffic security via microsegmentation, allowing users and/or devices to carry their own "virtual network" setup as they roam.
- Configure RWG with micro-segmentation to separate devices into their own VLANs. Use RWG's automation to configure multiple VLANs simultaneously.
- Use software-defined policies to create separate zones for different types of devices or applications.
- Leverage RUCKUS SmartZone or the RUCKUS One controller policy enforcement capabilities to enforce traffic separation between micro-segments.
- Optionally, the RUCKUS SmartZone solution with Data Plane allows for the separation of the control plane, which validates and authenticates users, devices, and applications, and the data plane, which is responsible for encrypting and securing data in-transit. This separation enhances network security within a Zero Trust environment by providing greater granularity, flexibility, and reliability, with the control plane managed centrally by a trusted authority, while the data plane can be distributed across multiple encrypted nodes or locations.
- Implement a firewall or next generation firewall (NGFW) that allows or denies particular types of traffic between containers that are separated at the network level. Even if the firewall is used for perimeter security only, it is an important first step in protecting data, especially if other methods of microsegmentation, such as role-based/user-based segmentation are utilized.

Least Privilege Access

The concept of least privileged is a security configuration that resides within most enterprise hardware but may not be utilized effectively or correctly. The concept of least privilege is the idea that not everyone needs super user access to the network configurations, and even those that do need it don't need that level of access all of the time. Least privilege also involves policies and procedures that users follow to use the least number of privileges needed to get a task done, and only "upgrade" access as needed for more sensitive tasks.

RUCKUS's least privilege ZTA involves a combination of hardware, software, and configuration to enforce the right level of access at the right time. These steps include:

- Defining the types of roles and access needed within your network. If you already have this, then reviewing those and determining if they give too much/too little access for any role.
- Make changes to roles and privilege levels as identified from your review.
- When setting up a user's access to a device (or application), or a group of devices (or applications), set up a unique user account that only has the access level that person needs.
- It is also best practice to start a user off with the least amount of access needed and selectively provide more access as justified or provide the ability to temporarily upgrade access.
- Set up the ability to "upgrade" that access for those who have administrative capabilities; this capability can be supported in multiple methods, including having that person login and use a login with higher level access only when needed.
- Make sure to review and limit roles and access to sensitive parts of your network and have audit logging turned on to track access and actions within sensitive parts of your network.

Multi-factor Authentication

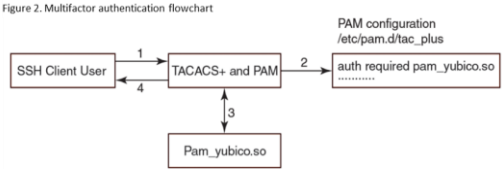
Multi-Factor Authentication (MFA) is a security control that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction, adding an additional layer of security, minimizing the risk of unauthorized access.

The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

RUCKUS supports multi-factor authentication at multiple levels accessing and within the network, and institutes checking for that authentication. Depending how your network is managed, controlled, and configured, your solution may vary, but could consist of some combination of these:

- RADIUS server configured to validate user credentials via multi-factor authentication to connect to the network.
- RUCKUS One configured to require MFA for any users of the RUCKUS One account for managing the network, using well-known authentication apps.
- Integrate Cloudpath solution into your network for authentication and onboarding, turning on MFA, and adding in a separate validation for third-party authentication via Google Authenticator, LinkedIn, or Facebook.
- Configure TACACS+ for use with ICX switches in your wired network for authentication, authorization, and accounting, and integrating the TACACS+ server and Pluggable Authorization Module (PAM) to integrate with Google authentication or Yubikey, adding to the MFA already set up to access the wireless network and control and management via RUCKUS One.

Figure 2. Multifactor authentication flowchart



Network Visibility

Just important as validating that users or devices (or applications) should be able to access different parts of the wireless or wired network is knowing what users are actually connected, have connected, or are able to connect. This is where network visibility enters into the ZTA solution.

RUCKUS provides numerous ways to gain visibility to users of the network, allowing views of usage, connections, data transfer, device stability, and many other things necessary for configuring and then maintaining the health of a network. Depending upon the solution, the granularity and ability to delve into the data for more analysis can vary. While RUCKUS doesn't provide a single viewing pane across all network and application events, it does provide deep visibility into network elements and events. Typical configurations can include a mixture of the following for full network visibility:

- RUCKUS One Professional with deep analytics and machine learning capabilities using real-time monitoring, device and user management and visibility, and visual network representation and modeling.
- Virtual RUCKUS SmartZone controller for control and management integrated with RUCKUS AI™, enabling real-time performance monitoring, unified wired and wireless policy enforcement, visual connection diagnostics, robust APIs for third party integration, and granular visibility and control over separate WLANs.
- Cloudpath solution to provide full listing of users/devices connecting to the network, real-time monitoring, and secure posture check to connecting devices.
- RUCKUS WAN Gateway (RWG) to provide real-time monitoring, detailed usage analytics, network visualization, and location-based services to allow for precise indoor tracking.

For end-to-end visibility, such as with a SIEM (Security Information and Event Management), RUCKUS allows the export of logs and other key information necessary for SIEMs to analyze data and manage events and incidents, as well as supplying APIs and MIBS that can be used within leading SIEMs to bring together a consolidated application, system, and network view.

Real-time Analytics and Automated Responses

Implementing policies, procedures, and controls for a ZTA requires access to data to report on and resolve real-world network situations. With real-time analytics, there can be proactive problem solving to identify and address issues, including security anomalies, before or as they occur. Performance of your network can be improved by identifying and removing bottlenecks or identifying misconfigurations. Security is enhanced when real-time analytics can detect and alert on suspicious network activity.

With RUCKUS, you get access to real-time monitoring as well as detailed analysis of network activity, a powerful combination to identify problems as they occur and identify problems that only appear by seeing network data over time. A typical RUCKUS solution would include:

- Control and Management utilizing RUCKUS One or virtual RUCKUS Smart Zone controller, allowing for real-time monitoring and alerting, helping to monitor network health and make changes as needed to improve network performance, add new devices, or resolve issues.

- Deep analytics utilizing RUCKUS One Professional or RUCKUS AI connected to virtual RUCKUS SmartZone controller, providing a wealth of data about network usage, including peak usage times, most accessed resources, and bandwidth consumption. This includes recommendations on what needs to be done to resolve issues.
- Cloudpath solution, to enable comprehensive visibility into network users, their devices, and their activities, helping IT manage network access, enhance security, and optimize network performance.
- RWG, improving visibility to device security, SD-WAN reliability, security vulnerabilities and threats, user activity and network issues.

Secure and Remote Access

Accessing the network remotely is now the normal for companies. This access can be done with company-owned or BYOD devices, but remote access still needs to be done securely. As part of a Zero Trust Architecture, the same type of authentication, posture checking, authorization, and verification must be done for remote users of the network. A typical configuration utilizing RUCKUS could include one (or sometimes more) of the following:

- Virtual Private Network (VPN) connection into the network. This VPN can be set up through the RWG or it can be another provider.
- SD-WAN provided via the RWG. SD-WANs allow for network-wide configuration that can be applied for multiple connections into the network.
- SASE provided by a third party. Just like with SD-WAN, it allows for network-wide configurations, but provides the benefit of being cloud-delivered. RUCKUS can provide the network at central and edge sites that is then securely managed with consistent secure access for users via the SASE.

Encryption

A Zero Trust solution also emphasizes the need to encrypt data to avoid security compromises. This is both data in-transit and data at-rest. In essence, Zero Trust emphasizes protecting data *wherever it resides*, because the complexity of networks continues to grow, leaving traditional mechanisms of protecting data at the end insufficient to ward off security threats.

RUCKUS employs encryption in its hardware and software products that help to protect data that is being transmitted through the network.

- RUCKUS Access points take advantage of the latest encryption capabilities such as WPA3, Dynamic PSK, and even hold FIPS 140-2 certification for select products for sale to US Federal customers.
- RUCKUS Switches employ AES Encryption (128/192/256 bit) with Secure Shell (SSH) v2, MACSec, and numerous other security controls.
- Cloudpath solution utilizes Digital Certifications, Dynamic PSK, and Secure Sockets Layer (SSL) to encrypt transmissions.
- RWG utilizes IPsec VPN and OpenVPN coupled with Customizable Key Exchange Frequency and Certificate lifetimes to enhance the security of data transmission via a “continuous verification” principle.

Policy Enforcement

Zero Trust relies upon the principle that every user, device, or communication must be verified. Policy enforcement means that, for each connection, that request is validated against a policy engine that determines the validity of the request and sends the result back to either allow or deny access.

Policy enforcement can be accomplished several different ways by leveraging the RUCKUS Networks approach to validating that users, both administrative and end user, should have access to networks, virtual networks, or network elements. The RUCKUS WAN Gateway acts as the policy enforcement engine and by being deployed on the network edge, it is uniquely positioned to act as the device implementing whatever policy the organization produces.

Sometimes, there may already be an existing policy engine to do policy enforcement; this can be integrated with the RUCKUS network to cover this crucial part of a Zero Trust strategy. Or, a customer can utilize a cloud-based or other policy engine and policy enforcement, leveraging RUCKUS products to provide the connectivity and security.

SOAR Technologies

Security Orchestration, Automation, and Response (SOAR) technologies allow real-time alerting, notification, automated workflow, and responses to security (or potential security) threats. Ideally, this collects data from across the entire network, from the access layer to within the network (behind the firewall) to identify potential security issues.

RUCKUS provides mechanisms for full network visibility, from the point of access control and entry to deep inspection of the network. Alerts, notifications, and remediation can be set up to address those areas of concern. A RUCKUS solution could include the following:

- RUCKUS One control and management with state-of-the-art AI and patented machine learning (ML) algorithms enabling IT to react quickly to incidents and prevent them from becoming service-affecting problems, classifying issues by severity, so IT knows where to focus first.
- RUCKUS AI in concert with virtual SmartZone, using powerful AI algorithms to automatically classify service incidents by severity—tracing root causes and recommending steps for remediation.
- Cloudpath solution, which provides visibility and control over users and devices on the network, with the power to

revoke access at any time, allowing for immediate response to any suspicious activity or identified threats as well as flagging and reporting devices that fail security posture checks.

- RUCKUS WAN Gateway, whose automated response system swiftly contains and isolates potential threats, minimizing the risk of data breaches and unauthorized access.

Conclusion

RUCKUS Networks takes the security of products, users, networks, and companies very seriously. Having a robust security capability for managing access, authentication, authorization, device management, visibility and event management, automated event logging with machine learning and AI built-in to flag threats and potential issues are all part of what is necessary to provide a secure and robust network solution. RUCKUS thinks about how users need to access the network, from the Edge inwards, logging into actual devices, onboarding new devices for the first time, and what level of roles and privilege are necessary to provide a functioning and secure network. RUCKUS has detailed configuration guides that provide best practices for designing, configuring, and securing your networks, all part of RUCKUS's approach to a Zero Trust Architecture.