ZTNA

WITH THE REVENUE EXTRACTION GATEWAY

rgNets

Zero Trust Network Architechture

Zero Trust (ZT) is a hot topic amongst information security professionals as it is widely promoted by industry research firms such as Gartner and Forrester. The ZT security model for information technology has been employed in various capacities to protect our digital world for over two decades. Standardization bodies such as the US National Institute of Standards and Technology (NIST) and the UK National Cyber Security Centre (NCSC) provide us with a clear and comprehensive understanding of zero trust with three core principles and five essential pillars to apply to information systems as well as the business processes that surround the technology.

The rXg is designed to be the head-end of a Zero Trust Network Architecture (ZTNA) that is part of a ZT security model deployment per the guidelines provided by formal documentation such as the NCSC Architecture Patterns for Zero Trust Networks and the NIST Special Publication 800-207. The ZT security model emphasizes strict access controls and continuous verification to ensure that only authenticated and authorized users can access digital assets. By relying on formal documentation from trusted sources such as NIST and NCSC, organizations can be confident that their security measures are effective and aligned with industry standards. In this context, we will discuss how rXg can help organizations deploy a ZTNA as part of a ZT security model implementation to achieve their security objectives by adhering to the principles outlined in NIST and NCSC documentation.

The rXg is more than just a solution, it's a game-changer for implementing a zero trust network architecture. With its powerful capabilities, the rXg empowers operators to seamlessly integrate the three tenets of ZT - continuous verification, least privilege implementation and automated response - across all five pillars to deploy a ZTNA in a reliable, scalable and cost effective manner. By deploying rXg, you can rest assured that your network is fortified against even the most advanced threats. The rXg's cutting-edge technology ensures that only authorized users and devices have access to your network, and that all network traffic is continuously monitored for any suspicious activity. This level of security and protection is essential for today's fast-paced digital landscape, where cyber threats are constantly evolving. Don't leave your network security to chance, trust rXg to safeguard your organization's most valuable assets.

THREE PRINCIPLES

- **Continuous Verification**
- **Least Privilege Implementation**
- **Automated Response**

FIVE PILLARS

- **Identity**
- **Device**
- **Network**
- **Workload**
- **Data**

Identity

The rXg provides a powerful and secure solution for network access, following the principles of the Zero Trust (ZT) security model. The rXg's internal identity engine, coupled with external directory services such as MSAD, RADIUS, LDAP, SAML, and OAUTH, enables compatibility with a wide range of sources, ensuring that only authorized users have access to the network. With the rXg, security is a top priority.

The ZT principle of "continuous verification" is a core feature of the rXg identity engine, allowing reauthentication at any desired interval and providing external triggers for identity reverification for added security. The rXg's identity engine seamlessly integrates with the policy engine, allowing automated packet filtering and forwarding decisions based on the ZT "least privilege" principle. This means that users are only granted access to the resources they require for their work, reducing the risk of unauthorized access.

Furthermore, rXg includes an automated response system that triggers re-authentication of identity in case of a breach, demonstrating its commitment to the principles of ZT security. This feature provides an additional layer of security, ensuring that the network remains secure even in the event of a breach.

The rXg's ZT security model also enables businesses to implement secure remote access, allowing employees to work remotely without compromising network security. The RXg's identity engine ensures that only authorized users have access to the network, while the automated response system triggers re-authentication of identity in case of a breach.

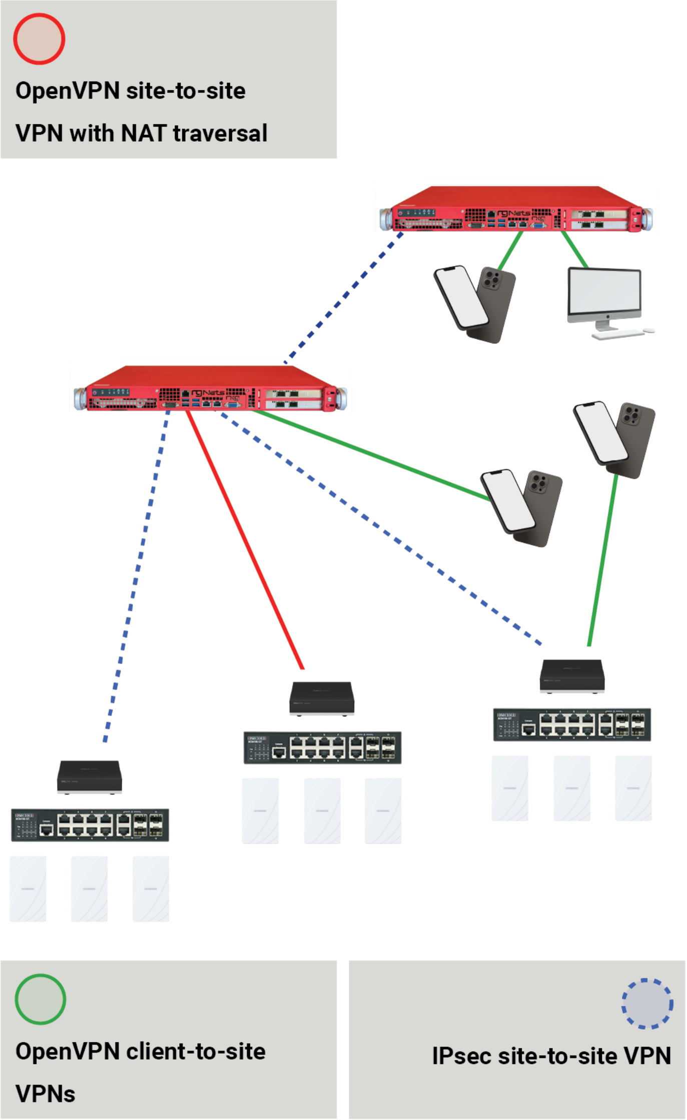
Overall, rXg's implementation of the ZT security model provides a powerful and secure solution for network access, ensuring that only authorized users have access to the network and that resources are only granted to those who require them for their work. rXg's commitment to security is evident in its seamless integration of the identity and policy engines, continuous verification feature, and automated response system. As such, the rXg is an excellent choice for businesses that prioritize network security.

Data

The rXg is a highly effective solution for organizations that require secure data transfer between locations, with exceptional security features that provide superior protection for data transmission. The advanced capabilities of rXg, including a high-performance, scalable, and comprehensive site-to-site and client-to-site VPN concentrator, make it an ideal choice for organizations that value data security and privacy. With its advanced VPN capabilities, rXg ensures that data is encrypted and protected during transmission, supporting both IPsec and OpenVPN protocols, and allowing for customizable key exchange frequency and certificate lifetimes to implement the ZT "continuous verification" principle.

In addition to its VPN capabilities, rXg also implements the ZT "least privilege" principle by deeply integrating with the micro-segmentation aware router and NAC features. This allows for requiring individual VPNs for accessing each application that routes through rXg, adding an additional layer of security. With rXg, organizations can ensure that users are granted access only to the resources they require for their work, ensuring that sensitive data is protected at all times.

The VPN concentrator in rXg can be configured in mass deployment scenarios via the rXg Fleet Manager, making it easy to deploy and manage across multiple sites. This feature reduces the complexity and cost of managing a VPN infrastructure, making it more accessible to organizations of all sizes. The rXg also implements the ZT "automated response" principle through automated disconnection of VPNs based on specific events, further enhancing the security and protection of the system. This ensures that any security breaches are quickly detected and resolved, minimizing the risk of data loss or unauthorized access.


OpenVPN site-to-site VPN with NAT traversal
OpenVPN client-to-site VPNs
IPsec site-to-site VPN

Overall, rXg provides a highly effective solution for organizations that require secure data transfer between locations, with exceptional security features that provide superior protection for data transmission. Its advanced VPN capabilities, customizable key exchange frequency and certificate lifetimes, micro-segmentation aware router and NAC features, and automated response system, make it an essential tool for any organization that values data security and privacy.

Device

The rXg incorporates advanced security features, including device posture analysis, as a critical component of the ZT security model. By leveraging data from multiple sources, such as passive fingerprints, active scans, and persistent software agents, the device posture analysis engine provides a comprehensive and dynamic evaluation of each device. This approach ensures that only trusted and secure devices are granted access to the network, helping to protect against potential threats.

To further enhance security, rXg implements the ZT principle of “continuous verification” on the device posture, allowing for real-time monitoring and updates at any desired interval. This continuous monitoring enables the identification of any changes in device posture, providing an additional layer of protection against potential threats. The rXg NAC engine seamlessly integrates the results of the posture analysis to assist with segmentation decisions and automate the enforcement of the ZT “least privilege” principle. In the event of a security breach, rXg’s automated response system ensures that only trusted devices are granted access to sensitive network resources, while potential threats are isolated and contained. These features demonstrate rXg’s commitment to providing a secure and robust network environment in line with the principles of ZT security.

Workload

The rXg offers a comprehensive security solution for your network infrastructure. With its advanced heuristic network behavior analysis engine and signature-based deep packet inspection engine, rXg provides real-time protection against a wide range of threats, including malware, hackers, and other malicious actors.

One of the key features of rXg is its ability to leverage historical information to improve its security capabilities. By analyzing data from past network activity, rXg can identify patterns in client behavior, and anticipate where potential threats may arise. This allows rXg to implement the principle of “continuous verification” by configuring its network behavior analysis engine to recognize patterns of traffic that fall outside of normal activity, and take action accordingly.

The rXg uses the results of its analysis to implement the ZT principles of “least privilege” for access and to limit potential damage through “automated response.” This approach ensures that only authorized traffic is allowed, while potential threats are swiftly contained and isolated. rXg is also able to detect and respond to any security incidents in real-time, minimizing the risk of data breaches and unauthorized access.

In addition, rXg’s advanced features and capabilities make it a highly effective solution for securing your network infrastructure. Its robust firewall capabilities and VPN concentrator, which supports both IPsec and OpenVPN protocols, ensure that data is encrypted and protected during transmission. The rXg also provides powerful micro-segmentation capabilities, enabling ultra-high scale segmentation and integrating seamlessly with RADIUS NAS platforms to build a deeply segmented network architecture in support of ZTNA.

Enter the 6 digit OTP sent via SMS on your registrerd mobile phone No. xxx xxx 1234

Your OTP code for register to ABC is 569786. Please enter this code within 3 mins. (Ref: PHDT3D) 10.44

Overall, rXg is an essential tool for ensuring the security of your network infrastructure. With its advanced security features, including network behavior analysis and deep packet inspection engines, as well as its micro-segmentation capabilities and VPN concentrator, rXg provides real-time protection against a wide range of threats and allows you to implement the ZT principles of “continuous verification,” “least privilege,” and “automated response” for added security.

Network

The rXg's microsegmentation capabilities are a critical component of its network architecture. Microsegmentation is an approach to network security that divides the network into smaller segments, each with its own security controls, policies, and access controls. The rXg's advanced data plane capabilities enable ultra-high scale microsegmentation by providing granular control over network traffic at the packet level. This level of control ensures that traffic is only allowed to flow between authorized devices, minimizing the risk of data breaches.

The rXg's control plane features a microsegmentation-aware Network Access Control (NAC) engine, which operates in conjunction with integrated RADIUS NAS platforms to enforce dynamic, policy-driven access control. The rXg NAC engine creates a deeply microsegmented network architecture, which is essential for Zero Trust Network Access (ZTNA). By implementing ZT principles such as continuous verification, rXg ensures that only trusted devices are granted access to the network. Onboarding VLANs and admission timeouts help to establish the trust level of devices, and quarantine and enrollment segments are automatically created and controlled by the rXg to provide additional security. The rXg's implementation of the ZT principles of "least privilege" and "automated response" further enhance the security of the network. Per-device VLAN enforcement ensures that each device is assigned a unique L2 VLAN and L3 /30 subnet, enabling individual control of privileges. This approach contains any potential breaches to the device segment, preventing them from spreading throughout the network. The rXg also implements automated responses to specific events, such as automatically disconnecting VPNs to ensure the security and protection of the system.

Overall, rXg is an essential tool for building a microsegmented network architecture that meets the needs of organizations with complex security requirements. Its advanced data plane capabilities, microsegmentation-aware NAC engine, and implementation of ZT principles ensure that only authorized devices and users have access to the network and that potential security breaches are contained and responded to automatically.

www.rgnets.com
sales@rgnets.com
316 CALIFORNIA AVE
RENO, NV 89509

–• –• – – – –• – • –• – – – • –•• / –• –• – – – – – – – •• – –• •• –
• –• • – – •• – – – –• / –• –• – – – – –• –• •• – –•• • – –• –• –• •