turnium
TECHNOLOGY GROUP INC.

TURNIUM SOLUTION BRIEF

Turnium Secure Networks: Three SD-WAN Architecture Types for Higher Resilience and Better Security

Software-defined wide area networking (SD-WAN) has become widely accepted as an architecture that enables secure communication between organizational sites as well as built in resilience and reliability. Turnium's SD-WAN offers three additional architectures that can deliver higher degrees of network security for customers. In these architectures, customers host all Turnium SD-WAN infrastructure in their own private infrastructure.

These architectures build on the classical concept of the "air-gapped network." An air-gapped network is one that has no network interfaces, either wired or wireless, directly connected to outside networks such as the Internet. This separation enables IT to implement a higher level of security across networks that transmit sensitive data. In today's business environment, it is increasingly important to protect networks from eavesdroppers and those who would steal sensitive data.

You network security needs can’t be ignored

IT security is commonly thought of in terms of protecting desktop and laptop computers and handheld devices. While this is true, your network is just as much a target for hackers because it provides unfettered access to all data and devices. This means that all nodes through which your traffic passes must be under your control and in your physical environment, and subject to your best-practices-based security policies.

Common wide area network (WAN) practice is to connect multiple sites using a VPN over the public Internet – also known as “tunneling” because the encryption provides a metaphorical tunnel through which data can flow confidentially; site-to-site traffic sent over the Internet is encrypted using your security policies. However, data that is destined for an address on the public Internet does not get encrypted – a configuration called “split-tunneling” – and is thus vulnerable to prying eyes. Worse, the inbound traffic from the public Internet can contain vectors of attack that can compromise your entire WAN.

Turnium SD-WAN architectures help secure networks

Organizations need a way to securely network multiple sites in a cost-effective fashion that fits your security governance model. Turnium’s SD-WAN solution can be architected in three different ways to meet the various network security needs of your security governance while not breaking the bank.

Pure Air-Gap

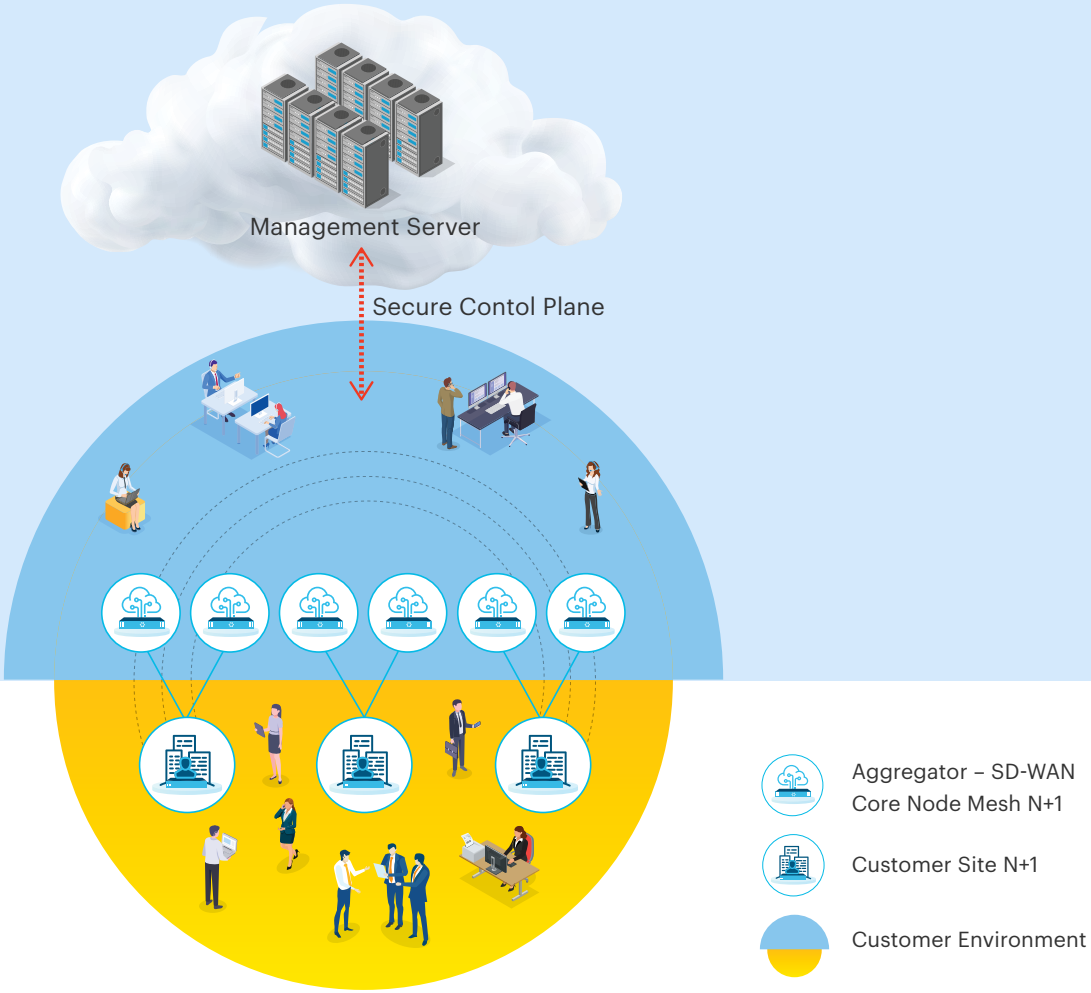
The most secure network architecture to deploy Turnium SD-WAN (barring breaches due to social engineering and human vectors) is one that is completely air-gapped, meaning that none of its internetworking equipment has a port that connects to another network. This requires that the organization provision private site-to-site links to transmit and receive data between sites. Multiple, leased, or privately-owned fiber or wireless circuits would be deployed at each site for business continuity and security.

In this architecture, Turnium SD-WAN and all component links, core nodes, edge nodes, Turnium Management Server (the control plane for the SD-WAN) and internetworking hardware is controlled, hosted, and managed entirely by the customer organization. This enables total separation. All data being transmitted over the SD-WAN is encrypted and the data obfuscated by distributing packets over multiple circuits at each site. This mitigates man-in-the-middle intercepts. By default, technical support would be conducted solely on-site or via telephone that is not connected to the network.

Air-Gap with Secured Control Plane Support

A second architecture to protect networks using Turnium SD-WAN is to deploy the same network and hosting architecture as in the Pure Air-Gap solution, but to provision a direct out-of-band (OOB) connection to the Turnium Management Server hosted by the customer organization for support and updates. An example could be the Management Server residing in a DMZ with controlled access to the server from the outside from defined ports or addresses. This enables Turnium's Technical Support Engineers to get visibility to the Management Server for support and updates.

As in the Pure Air-Gap design, all data in-transit is encrypted and distributed across multiple private, leased or owned wired or wireless circuits at each site. Packets from the data stream at each site are encrypted and distributed across the multiple circuits, obfuscating the data, and preventing man-in-the-middle intercepts. No corporate LAN or WAN data flows over the OOB connection to the Turnium Management Server as it acts solely as the control plane for the SD-WAN network. As the Management Server is only reachable through a separate circuit, the security benefits of an air-gapped network architecture are preserved.



Customer SD-WAN Deployment in Multi-tenant Management Server

This third architecture provides access to the network nodes through a secure control plane and provides security as well as offsite redundancy for the management server. In this design, encrypted network tunnels exist between the customer environment and the cloud-based management server. This architecture is not “air-gapped” but provides encrypted access to the network nodes through a secure control plane and provides offsite redundancy for the Management Server.

In this Turnium SD-WAN architecture the core and edge nodes and any other internetworking devices remain privately hosted by the customer and data in-transit is encrypted and obfuscated over multiple private or leased circuits. However, the Management Server or control-plane is hosted in a public cloud.

This design is useful when data sovereignty is required (e.g., personally identifiable information under GDPR or personal health data under HIPAA) and the core nodes and customer sites must remain within a specific jurisdiction, but the SD-WAN needs to be managed from outside of the jurisdiction. The Management Server can be in the Cloud or in a Turnium Partner’s data center as no customer data leaves the SD-WAN and there is no traffic through the Management Server other than the secured, encrypted control plane from the Management Server for control, configuration, and reporting data.

Summary

Regardless of which air-gapped network architecture you choose, Turnium SD-WAN enhances the organization's security posture by leveraging a combination of encryption, obfuscation, and physical control of the network which in turn simplifies the implementation of an organization's governance and security policies. Best of all, these architectures don't require expensive hardware or specialized skills and can be deployed over any circuit type.

About Turnium

Turnium Technology Group, Inc. delivers its software-defined wide area networking (SD-WAN) solution as a managed cloud-native service and as a white label, containerized, disaggregated software platform that channel partners host, manage, brand, and price. Turnium SD-WAN is available through a channel partner program designed for Telecommunications Service Providers, Internet and Managed Service Providers, and Value-Added Resellers. **For more information, contact** sales@ttgi.io.

About SD-WAN

SD-WAN is revolutionizing the networking and telecommunications industry by virtualizing secure, high-speed networking and abstracting network control from the underlying physical circuits. SD-WAN frees enterprises, small-medium businesses, cloud and managed services providers from the constraints imposed by traditional telecommunications companies.

turnium
TECHNOLOGY GROUP INC.