Empower Remote Workers with Secure Connectivity: DIA, Umbrella Auto Tunnel, and DVTI in Action

In this chapter, we delve into the practical application of using DIA, Umbrella auto tunnel, and DVTI. The use case details the scenario, network topology, and the end-to-end procedure for seamless implementation.

Enhancing Connectivity and Security for Remote Workers with DIA, Umbrella SASE Auto Tunnel, and DVTI

In today's interconnected and remote work environment, organizations face the challenge of providing seamless connectivity, secure access, and optimized performance for their distributed workforce. This use case explores the implementation of DIA (Direct Internet Access), Umbrella SASE auto tunnel, and DVTI (Dynamic Virtual Tunnel Interface) technologies to overcome network connectivity issues, enhance collaboration, protect sensitive information, and empower the remote users to work efficiently from any location.

Is This Use Case For You?

The intended audience for this use case is IT professionals, network administrators, and decision-makers responsible for managing and securing the network infrastructure, as well as organizations looking to optimize connectivity and security for their remote workforce. It provides insights into the implementation of DIA, Umbrella SASE auto tunnel, and DVTI technologies and highlights the benefits they offer in addressing the challenges faced by remote workers.

Scenario

Sally works as a remote sales representative for a global company that relies heavily on real-time collaboration and data access. She frequently travels to different client locations, but faces challenges in accessing sales data and communicating with colleagues.

What is at risk?

The company's existing network infrastructure is unable to provide seamless connectivity and secure access across multiple locations, resulting in delays, data inconsistency, and communication breakdowns.

How does a solution consisting of DIA, Umbrella auto tunnel, and DVTI in a hub and spoke topology solve the problem?

To address the challenges faced by remote workers like Sally, her company implements a comprehensive solution using DIA, Umbrella SASE auto tunnel, and DVTI.

1. **DIA:** DIA allows Sally to connect directly to the internet without routing through the corporate network. This provides her with faster and more reliable internet access, enabling quick access to cloud-based applications and services. It offloads network traffic from the corporate network, reducing congestion and optimizing performance.

2. **Umbrella Auto tunnel:** By leveraging the Umbrella Auto Tunnel configuration, Sally's company ensures that uniform security policies are applied to traffic regardless of whether Sally is remotely connected or behind a branch firewall. It eliminates the need for manual configuration of VPN connections and reduces the complexity and potential errors associated with traditional tunnel setups. This technology offers simplicity, convenience, and enhanced security for Sally and other remote workers in the organization

3. **DVTI:** DVTI in a hub and spoke topology enables the dynamic creation of secure IPsec tunnels between the branch office and the corporate network. These tunnels encrypt data transmission, ensuring secure access to corporate resources while working remotely. DVTI also optimizes network performance by intelligently routing traffic through the most efficient path and providing redundancy for uninterrupted connectivity.

By combining DIA, Umbrella SASE auto tunnel, and DVTI, Sally's company enhances her connectivity, security, and productivity as a remote worker. She can access cloud applications quickly, collaborate seamlessly with colleagues, and enjoy a secure and reliable connection to corporate resources, regardless of her location. The IT team benefits from centralized security management, reduced network complexity, and improved visibility into remote workers' activities.

Topology

In this topology, the internal client or branch workstation is labeled as WKST BR that is connected to the branch threat defense labeled as NGFWBR1. The headquarters threat defense is labeled NGFW1. The corporate network is reachable through NGFW1. The ingress interface of NGFWBR1 is named inside and the egress interfaces are named outside, outside2, and outside3 respectively.

A Umbrella auto tunnel is configured between NGFWBR1 and Cisco Umbrella.

All DNS and web traffic is sent through the Umbrella auto tunnel to Cisco Umbrella to be allowed or blocked based on the Umbrella DNS and web policy. This provides two layers of protection, one locally enforced by the Cisco Secure Threat Defense and the other cloud-delivered by Cisco Umbrella.

For the hub spoke configuration, a VPN tunnel is configured between NGFWBR1 and NGFW1. An ECMP zone is configured on the primary and secondary static VTI interfaces on the branch node for link redundancy and loading balancing of VPN traffic.
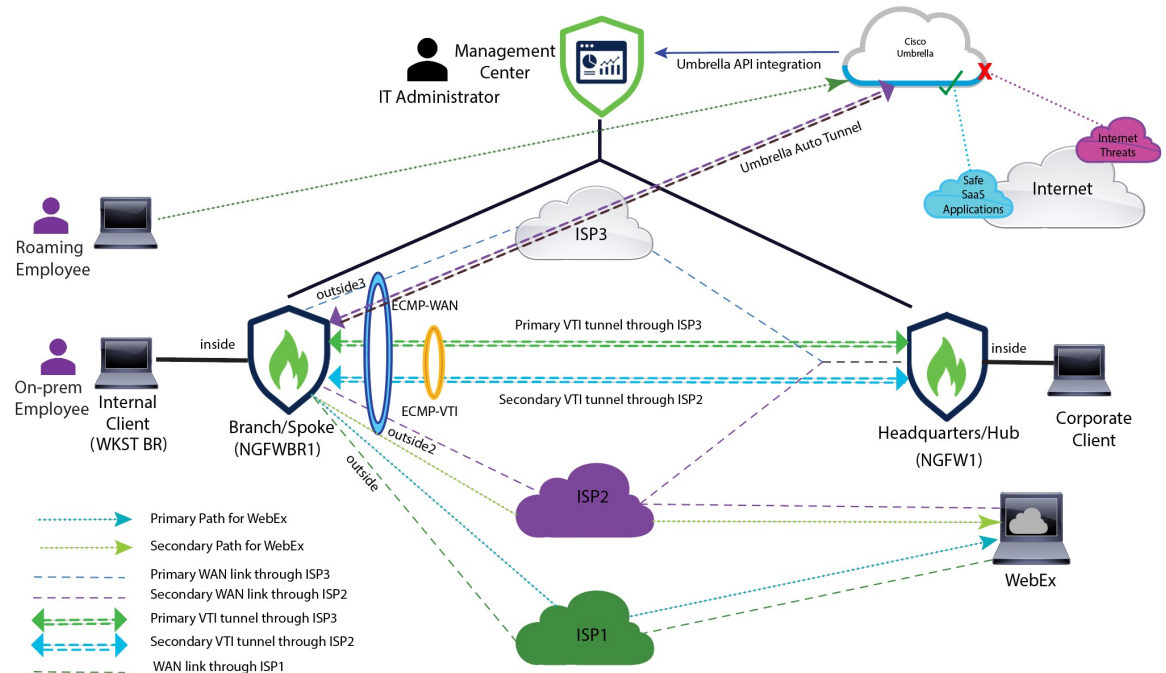
End-to-end Procedure for Configuring DIA, Umbrella Auto Tunnel, and DVTI

To configure the solution with DIA, Umbrella SASE auto tunnel, and DVTI:

- **Configure Direct Internet Access**: End-to-End Procedure for Configuring DIA With Path Monitoring

- **Configure Umbrella SIG Auto Tunnel**:End-to-end Procedure for Configuring Umbrella Auto Tunnel

- **Configure DVTI Hub and Spoke Topology**: End-to-End Procedure for Configuring a Route-based VPN (Hub and Spoke Topology)

Additional Resources

Resource	URL
Secure Firewall Threat Defense Release Notes	https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html
All New and Deprecated Features	http://www.cisco.com/go/whatsnew-fmc
Secure Firewall on Cisco.com	http://www.cisco.com/go/firewall

Resource	URL
Secure Firewall on YouTube	https://www.youtube.com/cisco-netsec
Secure Firewall Essentials	https://secure.cisco.com/secure-firewall