Sample Use Cases

For supported software information, click here.

This article provides sample use cases for the different Versa licensing solution tiers.

Use Cases for Pro Net Tier

The following tables provides sample use case scenarios for the Pro Net solution tier.

Target Use	Description
- Small branches with multiple circuits and deployments with backup option - Medium or large branches with a single circuit per box in a fully redundant box deployment - Any topology	Provides SD-WAN controller-based dynamic and encrypted connectivity, including extensive address translation options, for small branches **Capabilities** - Ability to set up dynamic IPsec VPN overlays that are transport agnostic - Address translation - Traffic steering based on routes and routing policies **Deployment Targets** - Small businesses with a single active link, hub-and-spoke topology, or without security; for example, branches connected to an MPLS VPN - Medium and large businesses with any topology, deployed across WAN links
- Small branches with multiple circuits and deployments with backup option - Medium or large branches with a single circuit per box in a fully redundant box deployment.	Extends SD-WAN functions by providing built-in core security features to leverage internet connectivity options in a secure and hardened environment Provides advanced load-balancing functions required for

Target Use	Description
• Any topology	third-party VNF chaining, for example, for WAN optimization and proxy. Provides application-level visibility with routing-level traffic policy control. **Capabilities** • Standard firewall capabilities provide base-level security capabilities for internet and other public networks • Single or multiple active WAN links, with LTE backup • Traffic steering based on routes and routing policies **Deployment Targets** • Small and medium businesses with base security; for example, fast-food restaurants • Deployments with direct internet access (DIA)
• Multiple active circuits for hybrid connectivity, application-based traffic steering, and monitoring • Hub sites that connect many branches or provide connections between data centers	Provides built-in core security functions to leverage internet connectivity options, topologies and protection. Provides advanced load-balancing functions required for third-party VNF chaining, for example, for WAN optimization and proxy. Provides application-level visibility with routing-level traffic policy control. **Capabilities** • Support for multiple active links • Application-based traffic steering, QoS, and monitoring **Deployment Targets** • Medium and large businesses with multiple active links; links can be hybrid (VPN + internet) or alike (VPN + VPN, internet + internet) • Application-based traffic steering and monitoring options • Application-level SLAs and monitoring, optimized for best voice and video experience

Target Use	Description
	• Single-box or dual-box deployments • Fortune 500 enterprise branch or metro offices • DC and hub site deployments.
• Advanced routing for vCPE, SD-WAN, and other router use cases, for physical and virtual deployments	Provides extensive routing, adding support for advanced protocols for routing deployments by service providers and Fortune 500 enterprises. Expands the routing foundation to enable security and SD-WAN use cases. **Capabilities** • Virtual routers with IGP, BGP, unicast IPv4/IPv6 forwarding, QoS, and IPAM capabilities **Deployment Targets** • Virtual route reflector and virtual router deployment in a data center • Virtual or bare-metal deployment in customer premises or service provider edge • MPLS VPNs, multicast, and segment routing capabilities • Virtual PE and virtual data center edge deployments involving VPNs • Public network (edge) deployments without built-in security or IPsec tunnels (IPsec transport)

Use Cases for SD-WAN Tiers

The following tables provide use case scenarios for the Prime SD-WAN, Prime Secure SD-WAN, Premier Secure SD-WAN, and Premier Elite solution tiers.

Next-Generation Firewall (NGFW)

Target Use	Description
• Secure cloud router with DoS protection and TLB	Core set of security features for a variety of deployments

	applicable for various branch, network edge, and data center use cases
	Capabilities
	- Advanced routing
	- Standard security using Layer 4 stateful firewalls and DoS protection
	- IKE-based IPsec VPNs for encrypted overlay tunnels
capabilities - Standard firewall with DoS capabilities - Secure cloud connectivity with intermediate-level security - Small branches and secure routers	**Deployment Targets**
	- Private and public cloud secure edge router deployments requiring IPsec VPN tunnels and advanced routing and VPN features with security
	- Secure data center perimeter and edge deployments with Layer 4 to Layer 7 TLB capabilities, together with standard firewall and DoS protection of data center and network assets
	- Single tenant and multitenant branch deployments with security and advanced routing functions, including overlays
	Application-based security capabilities to recognize an application's flows and applies security policies based on the knowledge and characteristics of each application
	Capabilities
	- Standard firewall
	- Application-level security
- Cloud routers with application security and IPAM - NGFW with application-level security and user control - Advanced security and routing for medium and large branches	- URL filtering
	- User and group policies
	Deployment Targets
	- Cloud and perimeter security roles, together with advanced routing capabilities, including TLB and DoS protection for data center servers and network assets
	- Advanced secure-router deployments in public and private cloud environments.

	• Multitenant, medium and large branch deployments with advanced routing and security capabilities and with IPsec overlays

Unified Threat Management (UTM)

Target Use	Description
• Advanced cloud routers with full security suite • Advanced firewall with application and content security, and PAM and UTM capabilities	Content (payload) inspection and security capabilities, scanning the packet payload and matching it with known vulnerabilities, viruses, and other malicious code or content **Capabilities** • Advanced NGFW with content security, IDS/IPS, and antivirus features **Deployment Targets** • Highly secure public and private cloud deployments and medium and large branches that require fully advanced perimeter security functions

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Licensing Overview