Versa Titan Solution Overview

Introduction

Enterprises are undergoing a digital transformation and as part of this transformation, the Enterprise WAN network raises a key challenge. The users have become hybrid and the applications are hosted in cloud networks or in on-premises datacenters. Cybersecurity attacks are also on the rise and threat actors are increasingly using advanced techniques to target enterprises and their data. The challenge faced by the IT team is to enable this digital transformation but also keeping the network secure from threats. IT teams in many small and medium size enterprises are lean and may not have dedicated network and security resources. The need to manage and train on multiple vendor products and management portals is a major challenge. What they require is a solution that helps them transform their network effectively, reduce the number of devices to be managed and at the same time offer a comprehensive security capability, all from a single pane of glass management and operations portal.

Versa Titan is a cloud-hosted Secure Access Service Edge (SASE) and Secure SD-WAN solution from Versa Networks. Versa Titan portal manages all of SD-WAN, security, routing and other functions from the cloud, making it easier for IT to deploy and operate their branch services and remote users. Powered by the market leading Versa Operating System (VOS), Versa Titan is easy-to-deploy, and best suited for lean IT and mid-market enterprises. Versa Titan enables enterprises to accelerate business growth as well as simplify deployment and administration. This enables a reduction in cost, time, and complexity associated with WAN transformation. Organizations gain enhanced visibility and control of applications, bandwidth utilization, network performance, and security threat prevention.

Versa Titan includes multiple access types, automated multi-path site-to-site VPN, direct Internet breakout to any cloud-based applications, ability to provide user and dynamic application prioritization, together with Next-Generation Firewall, Remote Access VPN, cloud hosted gateway based ZTNA, SWG and more. The Titan portal is available in eleven languages which Include English, Spanish, Mandarin, German, Japanese, Portuguese, Russian, Italian, Arabic, French, Turkish and Korean.

For MSP's, Versa Titan offers a comprehensive pre-packaged solution that allows them a single pane of glass view for all their enterprise customers. In addition, the MSP's can offer a SASE service for their enterprises where the SASE gateway can be either hosted and managed by Versa Networks or by the MSP in their own network.

Following are the key features of the Versa Titan solution.

- Context-aware enterprise grade SD-WAN & Security
- Secure Access Service Edge (SASE) services for ZTNA and Secure Internet Access
- Cloud-aware and SaaS accelerated solution for dynamic direct-cloud access
- Automated deployment for Lean IT
- Single pane of glass for management & analytics
- Pre-packaged enterprise portal for MSP's

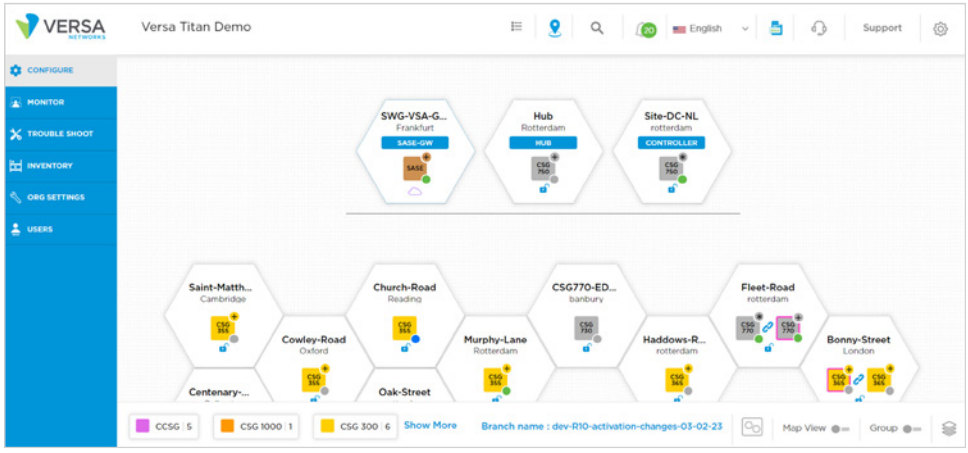

Figure: Versa Titan portal dashboard

Use-case - Lean IT approach for a Small Business Enterprise (SMB)

Background: A mid-size enterprise, ACME, manages a network of few hundred sites situated globally using a lean IT team. ACME has one vendor hardware used for WAN edge routing and another for security. ACME uses MPLS links to connect their sites to their datacenter and Internet links to access to cloud applications hosted in AWS and SaaS applications. The firewall on ACME's datacenter also functions as a remote access VPN server but the connectivity for remote users is poor whenever the bandwidth on the DC WAN links gets fully utilized.

The plan looking forward: The demand for bandwidth is growing as the number of users grow requiring capacity increase on network infrastructure, especially on WAN. At the same time, applications are moving to the cloud, hence traffic flow directions are changing from private DC to a mix of Internet and private DC bound. MPLS links are costly, and ACME does not want to invest more into MPLS to satisfy the growth need. Also, MPLS links may not be the best choice as applications are moving to SaaS providers. Hence ACME decide to completely remove MPLS links to be replaced with business class Internet connections over which SD-WAN will be used for WAN access. Hence the SD-WAN vendor solution needs to provide an enhanced application experience for all business-critical applications whether they are hosted on-premises, on public cloud or SaaS based. ACME also adapted a hybrid work policy with several users connecting remotely. Remote users need the same level of access as a user connecting from a branch site while connecting through a solution that provides modern ZTNA protections. Security is also of paramount importance, and ACME would like all user traffic whether accessing an on-premises application or cloud hosted apps to be inspected by comprehensive firewalls and get scanned for threats. This also means, Internet browsing traffic should be decrypted and inspected for threats. ACME IT team would prefer to have a solution that covers all of these needs in consolidated form to avoid complexity, cost and overhead of dealing with multiple products, vendors. Single pane of glass for SD-WAN, Security and Remote Access is required.

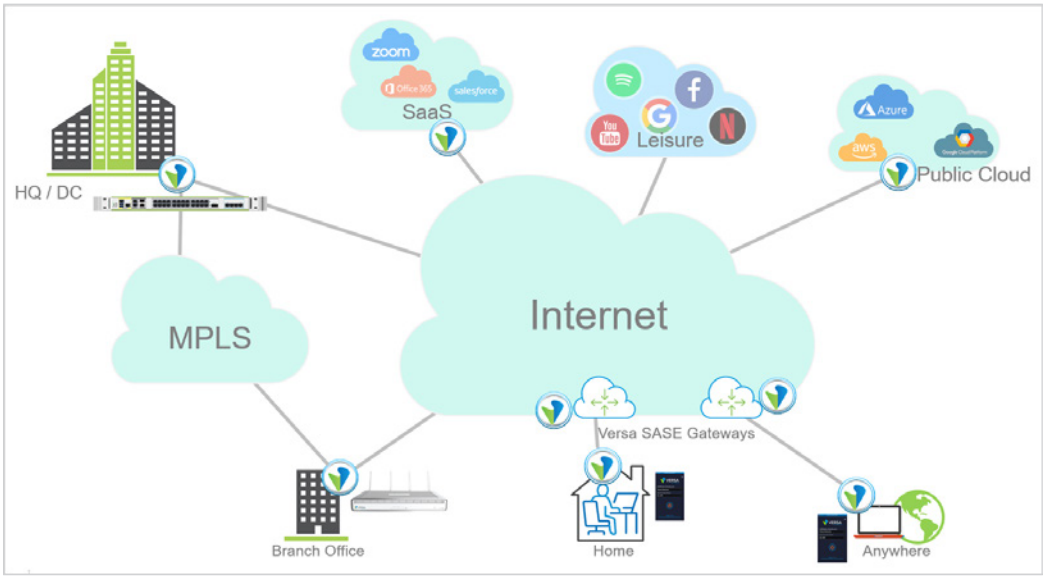

Figure: Enterprise migration to Versa Titan

Versa Titan with its advanced SD-WAN, Security and SASE services available in a single pane of glass portal, is a perfect fit for ACME enterprise. The IT team of ACME has been able to migrate its sites to an SD-WAN network at a fast pace with users benefitting from an enhanced application performance both for on-premises applications and cloud-based applications. The IT team is reporting lesser issues for remote users as they connect to the Versa SASE gateway and are not choked by bandwidth constraints at the DC. The savings in cost are visible as the MPLS WAN links on the sites are replaced with business grade internet circuits of higher bandwidth. With the Monitoring and Analytics capability, the IT team of ACME is better able to visualize the user traffic patterns and plan for network and bandwidth upgrades. The IT team has been able to use the security features of Versa Titan to ensure that all user traffic is effectively scanned for threats and malwares. The IT team at ACME has benefitted immensely from a simplified portal that can manage multiple services, it has helped them shorten their learning curve, be more efficient with the available resources and focus their efforts on offering a better service for their enterprise users.

To summarize, the benefits that the ACME enterprise gets with the Versa Titan solution include the following.

- Single pane of glass management portal for SD-WAN, Security and SASE service
- Advanced Traffic Steering capabilities for on-premises, cloud hosted and SaaS applications
- Advanced Security capabilities for branch and remote users
- Cloud hosted SASE service for securing access for remote users for private and public applications
- Deep insights into the network with AI driven Analytics
- Hub-Controller option for deploying sites with MPLS as they transition to Internet only
- Easy migration from legacy WAN to SD-WAN with the Gateway mode
- Range of hardware to choose from with in-built LTE and Wi-Fi
- Easy to do configuration portal with a shorting learning curve
- Simple software licensing structure
- Lesser device and vendors to manage
- Leverage the benefit of automation with templates and API's
- More tools to easily troubleshoot the network when dealing with user complaints

Versa Titan - Ease of Deployment and Management

Versa Titan portal offers a simple and easy to use UI (User Interface) for deploying and configuring branch sites. ACME IT administrator can create a common configuration and save it as a template which can then be applied to multiple branch devices. Subsequent changes made to this template can be propagated to the branches that refer to this template for its configuration. ACE IT administrator can create any number of such templates as required.

ACME IT administrator must simply drag and place the appropriate license type In the Titan configuration portal dashboard to configure a new branch site. ACME IT administrator then fills in the details about the site like the site name, device name, address, topology, serial number, configuration template etc. Any additional configuration required on top of the template configuration is done and then the administrator clicks on the deploy button. This means that the device is now ready for its Zero Touch Provisioning Procedure to onboard to the enterprise VPN.

ACME IT administrator has the following options to choose when it comes to Zero Touch Provisioning (ZTP).

1. **Global ZTP:** This ZTP option uses a fully non-Involved Zero Touch Provisioning process. The requirement is that the device must be connected to the Internet with an IP address obtained via DHCP from the Internet provider. Once the device receives its IP address and other details, it automatically calls home to the Versa call-home server and authenticates itself based on pre-loaded certificates and the device serial number. As the device has been authenticated, the final configuration is applied to the device, and it joins the enterprise SD-WAN VPN network. The complete provisioning process can be tracked in real-time from the Titan portal.
2. **Wi-Fi based ZTP:** This process is also referred to as URL-based-ZTP as a Titan portal generated URL is used by the technician on-site to quickly administer the ZTP process. In order to administer this process, an on-site technician would connect the Versa appliance to the WAN network and his or her PC to the appliance via one of the LAN ports or by using built-in WiFi of the appliance. The Technician's PC will receive an IP address from the appliance via DHCP and now the ZTP URL provided previously by the Titan portal can be opened using the browser on the PC. Once the link is opened, the automated ZTP process will move to the activation stages using simple to follow instructions on the web page and get the unit provisioned very easily. The advantage of this procedure is that WAN IP address can be both statically defined or be obtained through DHCP.
3. **Bluetooth based ZTP:** The technician on-site needs to have the Titan mobile application installed on their mobile device. The application is available on Apple and Android app stores. Once the technician logs in to the mobile application, the appliance will be detected using Bluetooth. After the appliance is discovered, the technician can start the activation procedure from the app. The benefit of this approach is the appliance does not require Internet access to download its configuration as the configuration is received from the mobile app through the Bluetooth connection. In this procedure the device WAN address can be statically defined or be obtained using DHCP. Versa Titan mobile app provides additional visibility on the progress of activation and once completed, other operational parameters of the unit can be fully visible from the app, helping the technician on-premises more with additional verification tasks that may need to be fulfilled.

Versa Titan is built from ground up to provide an easy experience to Enterprise administrators. Versa Titan comes with predefined options which are backed by best practice templates and proven ways to Implement routing, SD-WAN, security, and other functions to make deployment, operations and configuration tasks very easy, yet robust.

Titan solution includes an EASY button in every section of the configuration menu. The purpose of this button is to revert the appliance configuration to the configuration of the template. EASY button can also be used to make changes in the master template and then to apply the template configuration to each appliance that references this template. Additionally, every time the configuration of the appliance is changed and published to the appliance; a snapshot of the configuration is created. Later, the administrator can choose to roll-back to a saved configured snapshot if required.

Versa Titan - Device & Network Topology

A single branch appliance can be configured to be in a stand-alone mode or in High Availability (HA) mode. In HA mode, a standard Ethernet based inter-connection can be used between two platforms to logically extend the WAN transport link from one device to another. On the LAN side, VRRP is the default option, but the administrator can choose to implement dynamic routing protocol options too, if required.

The Network topology of the VPN is determined on a per appliance basis. The administrator can choose from the following SD-WAN network topology models.

- **Full Mesh:** This is the default topology for every new site.
- **Hub Spoke:** This has several diverse types of topology models as described below.
  - **Spoke to Hub only:** The spoke sites can only communicate only with the hub site. Direct spoke to spoke device communication is blocked.
  - **Spoke to Spoke via Hub:** The spoke sites can communicate with the hub site and with the other spoke sites, but the traffic path is through the hub device. This topology is useful to keep the SLA paths from the spoke to a small number or to apply some services centrally at the hub like security and traffic Inspection.
  - **Spoke to Spoke Direct:** The spoke devices can communicate with the hub device and with the spoke devices. If the direct path between two spoke devices is not available, then the traffic can flow through the hub if there is a path available. This topology is useful to provide a backup communication path through the hub in a scenario where there is no common transport between the spoke sites e.g., one spoke site only an Internet link active and the other spoke site only has an MPLS link active.
  - **Hub Spoke with Regions:** This topology is also referred to as Spoke-Hub-Hub-Spoke topology. Every hub and its constituent spokes are placed in a region. The topology within the region is governed by the hub-spoke topologies mentioned above. The region hubs are peered between each other. The spoke traffic between regions must flow through the local hub, remote hub and then the remote spoke branch. The same path applies for the reverse traffic flow. This topology option can be used to partition a large network into more manageable regions.
- **Partial Mesh:** The topology configuration is always set on a per-site level. So, sites with different topologies mentioned above can be configured to have specific partial mesh topologies as desired.

Hub-Controller: Versa Titan has support for a hub that double duties as a Controller. Please recall that the Versa Controller functionality provides centralized Control Plane functionality for the Versa solution. Versa Titan comes with cloud hosted Versa Controllers to ease and enable rapid deployments for our customers. Versa Titan controllers are cloud hosted and only available over the Internet. In scenarios where the enterprise only uses a private MPLS service for the branch, a specific hub device can be designated to function as a hub-controller so that such branches with no Internet connectivity can also get provisioned and managed via centralized Titan portal via the hub controller. In cases where the branch sites have both Internet and MPLS WAN links, the presence of the hub-controller can still be beneficial in the event that the branch site may encounter a temporary brown-out condition where the Internet WAN link is not available and the MPLS WAN link is the only connection available.

Gateway: Gateways are used when an enterprise is migrating to the SD-WAN network and would have to maintain connectivity to sites and services that are not yet migrated to SD-WAN. Gateway is not a separate node or functionality within Versa Titan. Any site and WAN link can be designated to function as a gateway, providing most flexibility for Titan customers.

Gateway functionality allows the leaking of the SD-WAN VPN routes to the underlay network and vice-versa for seamless brownfield deployments. Another use-case would be to provide access services that are provided by the underlay service provider e.g., VOIP services.

Cloud Deployments: Versa Titan portal can be used to configure and manage the VOS software branch that is deployed in a private cloud network or In a public cloud providers network like AWS, Azure, GCP etc.

Versa Titan Configuration and Features

Versa Titan has a gamut of features all packed in an intuitive and easy to use portal. This ensures that enterprises of varied sizes and needs have the required capabilities to build a secure SD-WAN network that provides an enhanced user and application performance in addition to keep the network and the applications secure from cyberthreats.

We will classify the features and capabilities as shown below and provide a brief overview of them.

- Networking & Routing
- SD-WAN Traffic Steering
- Security
- Remote Access VPN
- Secure Access Service Edge (SASE)
- Monitoring, Operations & Management
- Versa Analytics
- MSP Portal

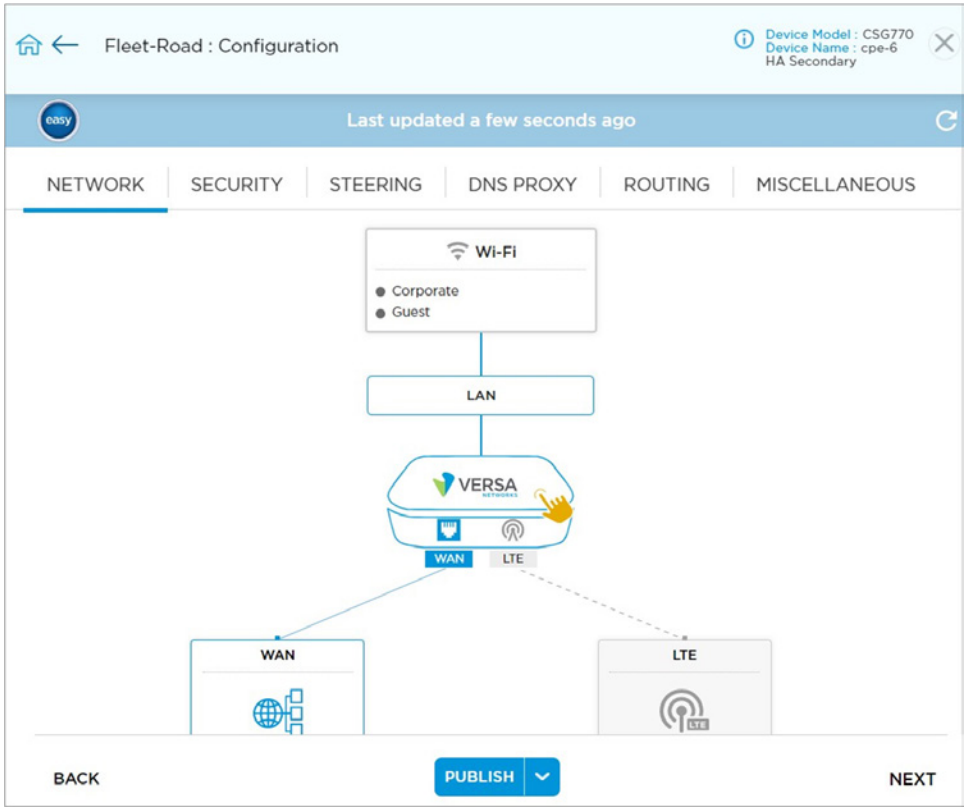

Figure: Versa Titan device configuration panel

Networking & Routing

WAN: The administrator can configure up to 4 WAN links on each device. The WAN links can be both Internet and MPLS circuits with support for VLAN's. IP addresses on these WAN links can be statically defined or be obtained through DHCP. Each WAN link by default is configured for VPN (SD-WAN) traffic and the Internet bound traffic, but this can be changed to make the circuit be dedicated only for the VPN traffic or only for internet traffic. PPPoE configuration is also supported as an additional option if required.

Depending on the hardware model chosen, the following WAN links can be configured.

- Ethernet
- xDSL
- LTE

LTE WAN links can be configured as Primary or in Standby mode. In Standby mode, they can be either in Hot Standby mode or Cold Standby mode. When configured as Primary, the WAN circuit is actively used for traffic along with the other WAN link. In Hot

Standby mode, the link is kept up but is only preferred as a link of last resort i.e., when all the primary WAN links are unavailable. In Cold Standby mode, the link is brought up only when all the other primary WAN links are unavailable.

LAN: Versa Titan supports a multi-VRF configuration which includes one Guest-VRF. A VRF stands for Virtual Routing Instance and is a logical router created in software that have its own IP interfaces and routing table. There is no exchange of routing information between VRF's. VRF routes between sites are exchanged over the Control plane channel and installed in the routing table. The Guest-VRF has no routes exchanged with other sites and only has a default route for internet access.

LAN interfaces on the appliance can be configured in Layer 3 only, Layer 2 bridge mode only or in combination. The latter is enabled with the use of IRB interfaces. IRB Interface gets mapped to constituent Layer 2 ports which then can be assigned to a VRF. Multiple LAN ports can be combined into a single LAG interface. VLAN sub-interfaces are supported on all Layer-3 interfaces. Layer 3 interfaces can be configured to function as a DHCP Server or Relay with support for DHCP client options. Port Forwarding (NAT) can be used to host a public facing application in the LAN network.

For loop prevention in the Layer-2 ports, RSTP and MSTP can be configured. To ensure that only trusted clients connect to the network, 802.1X protocol is supported on the LAN. This also makes Versa Titan an optimal choice for use-cases where a device needs to be setup for remote access because the clients connecting can be authenticated to ensure that there is no unauthorized access into the Enterprise VPN.

If the Versa CSG appliance model selected has built-In support for Wi-Fi, then there are multiple SSID's available that can be configured. For instance, one SSID can be configured for corporate Enterprise employees and the other for Guest Internet Access.

Routing Protocols: The Versa Titan supports static routes and dynamic routing protocols for the LAN and WAN interfaces. BGP and OSPF are the two dynamic routing protocols supported. The administrator can configure routing protocols in any of the VRF's. Connected routes and Static routes in a VRF are automatically advertised into the SD-WAN VPN network so they reachable from other sites.

BGP is a dynamic path vector protocol and is commonly used when exchanging routes on the LAN or on the WAN with the service provider. If BGP peering is configured on the WAN underlay network, to peer with the underlay provider's PE router and if the Gateway mode is set in Titan on the WAN interface, SD-WAN VPN routes would be automatically advertised to the Service Provider and the received underlay VPN routes are automatically propagated into the SD-WAN VPN network. On the LAN, any routes received from the BGP peer are automatically advertised into the SD-WAN VPN network. Routes received from the remote SD-WAN VPN sites are also automatically advertised to the BGP peer. The administrator can configure BGP policies to filter which prefixes are sent or received. In addition, the received routes can also be tagged with a BGP community value. BFD protocol can be used to detect peer failures and enable faster convergence.

OSPF is a popular protocol that is primarily used on the LAN. The administrator can define the area-id, password, and the interface on which the OSPF neighborship should be established. BFD protocol can be enabled with OSPF. The administrator can set a policy to block any routes that they do not want to be distributed from the SD-WAN VPN network into OSPF. Similarly, a policy can be applied to filter routes that the administrator does not want distributed from OSPF to the SD-WAN VPN network.

Versa Titan - SD-WAN Traffic Steering

Versa Titan has a fully featured SD-WAN traffic steering capability that ensures that the application takes the best possible path to ensure an optimal application and user experience. Irrespective of the type of WAN underlay circuit used, the administrator has the benefit of a policy driven approach that dealing with applications with distinctive characteristics and requirements. Versa Titan provides traffic steering capabilities not just for applications hosted on-premises but also for cloud SaaS based applications. If the user's pc has a PAC file for web proxy, the Titan administrator can configure a traffic steering rule to bypass the proxy and do a local breakout.

Titan's SD-WAN Traffic Steering configuration pane has a Rule and Profile section. In the Profile section, the administrator configures the SLA traffic steering conditions and, in the Rules, the configuration for the matching the traffic that should be steered is defined. Any number of profiles and rules can be configured as required.

On-Premises Applications

Under the Profile configuration section of Titan portal, the administrator configures the priorities of the WAN circuit paths. Then the circuit selection criteria also referred to as SLA criteria needs to be defined. If the criteria specified is breached, the application traffic

will move to the next WAN path of lower priority. If this path also does not meet the SLA threshold, the application traffic moves to the next path and so on till a path is found where the SLA criteria is met.

- Latency in msec
- Packet Loss in %
- Delay Variation (Jitter) in msec
- Mean Opinion Score (MOS)
- Circuit Tx Utilization in %
- Circuit Rx Utilization in %

The administrator can configure one or more of the above metrics in a Traffic Steering profile. The Latency, Packet Loss and Jitter have an option to select the lowest value, or a specific SLA value can be specified e.g., 2% Packet Loss. A Low value means that if there are more than one WAN paths available with the same priority then the system chooses the path with the lowest SLA value. The MOS refers to a scoring value from 1 to 5 which indicate the quality of a voice call or a real-time session. The Versa VOS appliance can compute the quality of the voice call in real-time and give it a MOS score that is used for traffic steering decisions.

Every Versa appliance computes the real-time SLAs to every remote site on every possible WAN circuit path. These measurements are used as the basis for traffic steering decisions. For every new traffic flow that matches the SD-WAN rule, the system checks if the SLA criteria is met on the path with the highest priority. If the SLA conditions are met then the traffic remains on this path and if not, it checks the SLAs on path with the next priority and so on. When it finds a path where the SLA conditions are met then the traffic stays on this path. If the condition of the path changes, for e.g., if the SLA conditions of the existing WAN path deteriorates or the SLA conditions of a higher priority WAN path improves then the traffic can shift to that path in real-time.

In the Traffic Steering profile, the administrator can configure the load-balancing algorithm when there is more than one path of equal priority. The default is to load share on a per-flow basis but can be changed to a per-packet basis if required. If all the WAN paths are out of SLA compliance, then the system can be configured to do a Loss recovery by either replicating the traffic flow on two paths or by sending a parity packet for every 4 data packets.

After the Traffic Steering profile is configured, the administrator configures an SD-WAN rule that defines which application and user traffic to match and then apply the traffic steering conditions that are defined in the profile. The traffic can be matched based on the following traffic match patterns.

- IP Protocol
- Source and Destination Zone
- Source and Destination IP prefix
- Hostname
- Application
- URL Category
- DSCP values
- Active Directory User and Group

When the traffic matches any of the conditions defined in the SD-WAN traffic steering rule, the WAN exit path is chosen based on the conditions defined in the SD-WAN profile. As part of the Rule action, the administrator can also define TCP optimization. TCP optimizations mitigate the effects of high latency and packet loss on the performance of TCP-based applications. The optimizations are based on a TCP proxy architecture.

Cloud Applications

Nowadays, an Enterprise's business applications are not just running on on-premises datacenters but more likely hosted in public cloud networks like AWS, Azure etc. and in SaaS clouds like Microsoft SharePoint, Salesforce etc. Such cloud-based applications can also be accessed through the Internet while Internet is a public network which does not provide any guaranteed SLA's. Versa Titan offers the possibility to host a VOS branch in the public cloud VPC or VNET thereby making the cloud network become another branch from an SD-WAN VPN network perspective availing all benefits of SD-WAN traffic steering. For SD-WAN best path selection to applications hosted in public SaaS clouds, this is done intelligently by monitoring all the available WAN circuit paths even if the WAN circuit path is not local to the device but available via a remote branch. The branch then combines all these metrics and chooses the best path for the SaaS cloud traffic.

The administrator can also configure a DNS proxy policy configuration that steers the traffic onto the same path on which the DNS request was sent. This is a matter of significance because every ISP in various locations would try and resolve the hostname query to an IP address that is closest to its geographic location. Having the steered traffic follow the DNS request ensures that the same ISP path is chosen that resolved the DNS query. In this case, when the DNS query is initiated from the client, the system first lookup

the SD-WAN policy to determine the best path it should take for this SaaS web traffic and steers the DNS query on that path. The system can choose between a local WAN path and a remote internet WAN path because sometimes a local WAN circuit might perform worse than the internet circuit WAN circuit of a remote site reachable over a private MPLS network.

Versa Titan - Security

Cybersecurity attacks are on the rise and security of the applications and the enterprise data is of paramount important and Versa Titan is built in with a complete Next-Generation firewall that enables this protection at the network layer. The traffic is scanned and protected irrespective of whether the user is accessing an application that is hosted in a private datacenter, public cloud provider like AWS, Azure etc. or hosted on the internet. The user is secured whether they are located behind a Versa Titan branch or connecting remotely. Irrespective of the location of the user or the application, the security of the network should never be breached and Versa Titan has a comprehensive security stack to enable this protection.

Versa Titan's natively built-in Next-Generation Firewall module allows the administrator to define policies that either allow specific traffic, block it or scan for threats. The traffic to be matched can be based on the following criteria.

- IP Protocol
- Source and Destination Zone
- Source and Destination IP prefix
- Hostname
- Application
- URL Category & Reputation
- DSCP values
- Active Directory User and Group

To enable user and group-based rules, the Versa Titan's firewall functions can be integrated with Active Directory using an LDAP, Kerberos or SAML. Once the traffic matches a rule, the action can be to allow the traffic, block it or further inspect it for threats. The firewall rule hits can also be logged to Versa Analytics.

For threat prevention, Versa Titan offers the following options that can be references in a firewall rule.

- URL Reputation & Categories
- Anti-virus
- Intrusion Prevention System (IPS)
- Geo-IP Filter

For ease of operations, Titan has three pre-defined profiles termed as Low, Standard and High. These pre-defined profiles are available in the URL based threat prevention, Anti-Virus and IPS sections. As part of the URL threat prevention module, the administrator can choose to customize which categories and reputation they want to allow in these pre-defined profiles. In addition, there is also option to configure an Allow and Deny list of URLs. As part of the Anti-Virus module, the administrator can choose whether to scan email traffic, web traffic or both. For IPS, Versa has several pre-defined profiles that the administrator can use in the configuration. Each of these profiles can have signatures that range from a few hundred signatures to several thousand signatures.

Most traffic on the internet today is TLS encrypted. For effective security scanning for threats, it is important that the Titan enabled appliance decrypts encrypted traffic so the HTTPS payload can be inspected. Versa Titan offers a full featured TLS decryption function where the administrator in the form of Rules can define which traffic to decrypt and which traffic to not decrypt. Versa Titan allows Enterprises to load their own certificates for TLS Proxy purposes.

Versa Titan - Remote Access VPN

Any Titan deployed branch site can be made into a remote access VPN device which allows a user located outside the Enterprise branch office to securely connect to the branch to access application and services located in the VPN network. Access is enabled through an IPSEC tunnel from the Versa Client App software Installed on the user's PC or mobile device.

Versa Titan - Secure Access Service Edge (SASE)

The need to securely connect users to the application is not limited to only users behind the branch office but also for users connecting remotely over the internet. Versa Titan offers a comprehensive cloud hosted SASE service in the Titan dashboard

portal thereby making it a single pane of glass for both Secure SD-WAN and SASE services. The SASE gateways can be hosted and managed by Versa Networks or by the MSP in their own network. The Versa SASE service offers the following two services.

- Versa Secure Private Access (VSPA)
- Versa Secure Internet Access (VSIA)

Versa Secure Private Access (VSPA): This service connects the remote users to the enterprise private applications. The user connects to the Versa cloud gateways using an IPSEC tunnel that is initiated by the Versa Secure Access (VSA) client installed on the user's PC or mobile device. It is important that the principles of Zero Trust Network Access (ZTNA) are implemented, and the user is authenticated prior to connecting to the enterprise VPN network. This can be by authenticating the user using LDAP or SAMP as an example. It is recommended that 2-Factor-Authentication (2FA) is turned on for additional security. Once the user connects to the gateway, the access to the application is either through an SD-WAN enabled IPSEC tunnel to the enterprise datacenter or through a Site-to-Site IPSEC tunnel. Connecting through an SD-WAN enabled tunnel has the added benefit that traffic steering policies can be used to ensure that the best possible path is chosen when reaching the Datacenter. Titan portal provides unified management capabilities for VSPA and other services a customer may be enrolled to.

The Versa Client App connects the user's PC to the gateway has a host of features included. Such features Include support for two factor authentication, remembering user credentials, always-on tunnels, tunnel monitoring and other whichh can be configured from the Titan dashboard itself. The Versa Client App has the capability to do a split-tunnel for traffic based on IP addresses but also based on application and domain names.

Versa Secure Internet Access (VSIA): The Versa SASE service offers protection for web traffic that is passing through the Versa SASE cloud gateways. The user can connect to the gateway using the VSA client, but the connection can also be made from a Versa SD-WAN enabled branch or any branch using a Site-to-Site IPSEC tunnel. All the Next-Generation Firewall features discussed earlier in this document are applicable as part of cloud-delivered VSIA service. Titan portal provides unified management capabilities for VSIA and other services a customer may be enrolled to.

Versa Titan - Monitoring, Operations and Management

The Versa Titan is a single pane of glass also covers monitoring of devices and services and facilitates network troubleshooting. In the Versa Titan portal, there is a separate section called Versa Titan Monitor where the health overview of all the sites in the network is shown with a color-coded bar indicates the health of each appliance. Within the Monitoring window, each appliance is an object which the administrator can double-click on to see detailed health status of all the services including network functions, security functions, and general device health. Device health status information like the status of the WAN links, status of site-to-site SD-WAN VPN connectivity, connected devices, device CPU utilization, device memory utilization, device disk utilization etc. Other monitoring information like WAN link utilization, applications used on the WAN links, routing table of the VRF's, web traffic denied etc. is shown. There is a separate section for device troubleshooting tools which have a wizard that guide the user to investigate a problem and has tools included like ping, traceroute and a speed test utility and an ability to do a configuration check. There is also option to obtain more detailed real-time monitoring information like the ability to view show commands from the various system modules and monitoring the traffic pattern in real-time.

For device management, SNMP can be configured on each of the devices where both SNMP v2c and v3 is supported. The logs from the appliance like device alarms and flow logging information from the firewall module are sent to Versa Analytics by default but the administrator can configure a syslog server to an external SIEM server for further analysis. Configuration audit logs are available on the Titan portal that the administrator can access. Upgrade of the appliance software can be done by the administrator from the Titan portal itself. If there is a faulty hardware, the process of replacing the device can be administered via the Titan portal while still maintaining the appliance configuration.

Support for Role Based Access Control (RBAC) allows the administrator to have different users on the portal but with different privileges. A set of users can have complete access to all configuration options while other users can have restricted access to the device configuration. Another set of users can be configured as an Operator which allows them access to deploy and monitor devices but not make any configuration changes. Even when providing configuration access, specific privileges like access to make configuration changes to sections like WAN, LAN, LTE, Wi-Fi, Security, Steering, etc. can be controller for users.

Note that as part of the Versa Titan offering, Versa Networks is responsible for ensuring the availability of the portal and the Titan service. This includes entire Versa Titan stack Including Versa Controllers, Versa Titan Portal, built-In Analytics and other required hardware and software Infrastructure elements. The management of the customer setup including branch and hub devices, WAN links, cloud branches etc. is the responsibility of the Enterprise or the MSP.

Versa Titan - Analytics

Versa Titan has built-in bigdata based analytics to provide rich historical and near real-time information about the network. Collected data can be viewed in the form of dashboards, charts, and reports. Versa Titan Analytics has a dashboard section and a log section. Dashboard covers highlights of SD-WAN, Security, Secure Access, and System. Several graphs and charts provided include WAN link utilization, SLA between sites on each WAN path, SLA violations, Quality of Experience Graph, Top applications, Top users, VRF usage, Top web threats detected, Top malwares found, Top applications based on risk, VSA user map, System CPU usage, Disk usage, Memory usage, Site availability etc. Customized reports can be created within the Reporting section of Versa Titan Analytics. Such reports can be scheduled to be created automatically at regular intervals to be emailed to the Administrator.

Versa Titan - Licenses and Hardware

The Versa Titan licensing has two components: feature tier and duration of subscription. During initial provisioning, first the feature license which is tied to the device hardware model is selected. There are the three feature tiers in which each tier focusses on addressing needs of certain deployment scenarios and use-cases.

- Enterprise
- Advanced Security
- Secure Application Optimization

Titan Enterprise license tier provides robust coverage of, Layer-2, Routing, QoS, SD-WAN and NGFW (Layer4-7 Firewall), User and Device Authentication, Web Filtering capabilities and more. These features enable enterprises to have comprehensive connectivity options within each site, across sites using SD-WAN capabilities, and to Internet while making use of L4 through L7 Security features.

Titan Advanced Security feature tier adds UTM and deep traffic and content scanning capabilities on top of the Titan Enterprise tier. Such deep scanning focused security capabilities include NG-IPS, Malware Protection, along with SSL/TLS Proxy capabilities.

Titan Secure Application Optimization feature adds application traffic optimization features on top of Titan Advanced Security tier. Titan Secure Application Optimization tier includes advanced features such as TCP Optimization, single sided traffic optimization capabilities such as DIA/DCA Traffic Optimization, DNS Proxy and DNS Assisted Traffic Steering, First Packet Based Traffic Steering capabilities for cloud based popular applications.

In addition, Remote Access VPN add-on option can be purchased to cover respective functionality. Remote Access VPN add-on entitles associated Titan branch appliance(s) to function as a Remote Access VPN server. This add-on license can be applied to any of the above three tiers.

The feature license is tied to the specific device hardware model. The following hardware models are supported in Versa Titan

- Versa CSG platform
- Versa Dell VEP platform

In addition to hardware appliances, Versa Titan allows hosting the Versa VOS software on any public or private cloud network. These licenses are referred to as cCSG and vCSG licenses. vCSG licenses are used for private datacenter based virtual appliances and cCSG licenses are used for popular cloud based virtual appliance deployments. vCSG and cCSG licenses come in three flavors, Medium, Large and XL. For SASE services, Versa Titan offers a license based on the number of user or bandwidth used. For SASE services, the user can purchase the Versa Secure Internet Access (VSIA) service and/or Versa Secure Private Access (VSPA) service.

All Titan licenses are time bound can be purchased as a 1-year, 3-year or 5-year license.

For more details about Titan licenses, refer to the Versa Titan datasheet.

Summary

Versa Titan is a cloud managed secure SD-WAN & Security service that addresses the needs of Lean-IT enterprises. In general, Lean-IT enterprises are most likely to be in SMB, SME, and mid-market segments across different industries. Lean-IT network operators may be best characterized as operators who may not see networking & security as their core competency and lean-IT networks operate their networks based on lean IT staffing, while the same IT staff may also be working on tasks outside of networking & security as well.

Versa Titan service comes with a cloud based, easy to use Titan portal. The Titan portal infrastructure is run by Versa Networks to provide rapid means to deploy and secure the enterprise VPN network. Enterprise benefit from a lower TCO when deploying with Versa Titan at the same time having access to a state-of-the-art solution with a plethora of features to address various deployment use-cases.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com