DATA SHEET

WAN Security

Overview

Ipanema's **WAN Security** function **simplifies hybrid WAN deployments.** Ipanema appliances protect your branch Internet connections from threats, **without using additional security devices in the branch.** With just a few clicks, you can enable your branch through your Ipanema appliance to access public and private datacenters. VPNs on IPsec or Generic Routing Encapsulation (GRE) can be terminated at the Ipanema appliance to encrypt traffic, which traverses the Internet. The Ipanema appliance can be easily configured to apply local **"allows/denies" to the Web traffic.** Additionally, these flows can be directed either through an access tunnel and secured by an **external Secure Web Gateway** (e.g. Zscaler before and after traversing the Internet backbone) or through a cloud hub exchange to accelerate S aaS applications.

Therefore, by coupling WAN Security to Application Visibility, Application Control and Dynamic WAN Selection (DWS), the hybrid WAN becomes a Next Generation Hybrid WAN solution (i.e. DWS + WAN Security), one that is secure, user-centric, scalable and offers dynamic path control. Ipanema Hybrid WAN automatically chooses the best WAN network path for each application flow, taking into account the real-time end-to-end performance of all trusted and untrusted available links. The Ipanema system maximizes the end-user experience and secures the use of all diverse WAN access technologies in your network.

By coupling WAN Security to Application Visibility, Application Control and Dynamic WAN Selection (DWS), the hybrid WAN becomes a Next Generation Hybrid WAN solution (i.e. DWS + WAN Security), one that is secure, user-centric, scalable and offers dynamic path control.

How Ipanema's WAN Security Works

Next Generation Hybrid WAN deployments use DWS to distribute flows over two or three WAN accesses. Consequently, DWS allocates bandwidth for every single flow given its priority and the state of every available path in the network. As DWS supports direct Internet links, in addition to MPLS or other WAN links, the customer flows are encrypted (AES 128, 256 or triple des) on IPsec VPN tunnels. The result is the ability to interoperate with a range of WAN connections, without the need for specialized security devices to terminate the VPNs at the branch location.

Branch offices can also be connected to local Internet connections by activating tunnels through a Secure Web Gateway. Direct-to-Internet rule exceptions can be defined as part of the security and policy strategy of the network. By default, the WAN interfaces deny all in/out traffic to traverse the Ipanema appliances toward untrusted WAN interfaces. You can activate exceptions to allow specific Web traffic to cross the tunnel and go to a Secure Web Gateway.

Ipanema SD-WAN, application intelligence for the WAN edge, links application performance over the network with the enterprise's business goals.

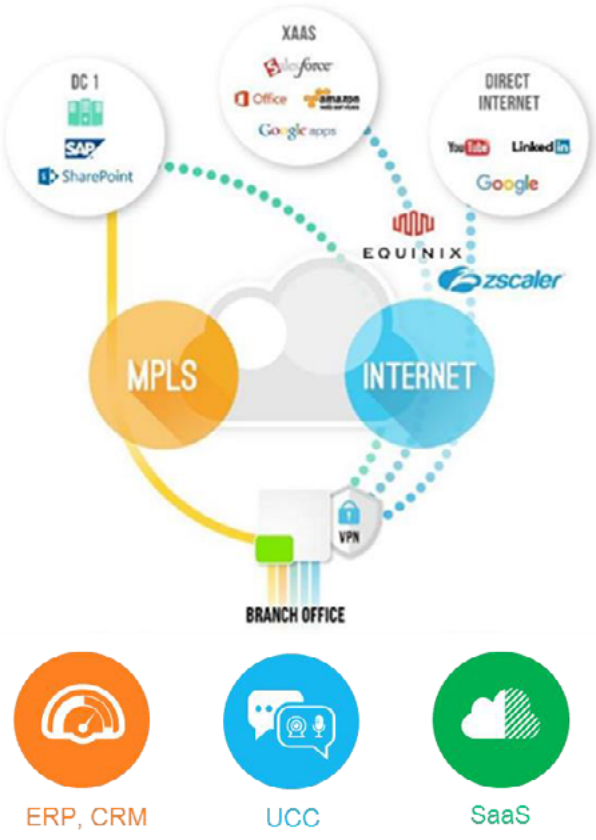
- **Self-learning, self-adapting and self-healing,** Ipanema offers tightly coupled features that bring a unique level of intelligence to the enterprise network;
- **Application Visibility** provides full understanding of application usage and performance over the global network – from the smallest detail up to SLA-based application performance management;
- **Application Control** dynamically adjusts network behavior and resources to the exact application traffic demand – guaranteeing critical application performance in the most complex and changing traffic situations;
- **WAN Optimization** accelerates application response times and offers additional virtual bandwidth to the network;
- **Dynamic WAN Selection** enables dynamic hybrid WAN for multi-networked branch offices, selecting in real-time the best path according to actual performance and application traffic characteristics;
- **WAN Security** protects branch Internet connections from threats. It encrypts traffic over IPsec VPNs to public and private DCs. It forwards Web traffic to Secure Web Gateway providers and allows/denies traffic to go directly to the Internet.

Next Generation Hybrid WAN deployments use DWS to distribute flows over two or three WAN accesses. The result is the ability to interoperate with a range of WAN connections, without the need for specialized security devices to terminate the VPNs at the branch location.

CONFIGURE WAN SECURITY

WAN Security is configured in conjunction with DWS. MPLS and other WAN links (e.g. Internet, LTE) can be configured in Full Dynamic mode or Primary/Backup mode. Full Dynamic mode means that the Ipanema system will measure the current performance of each WAN connection and will forward the traffic flows over the path that matches the predefined APO (Application Performance Objective). Primary/Backup can be also configured when the enterprise has specific resource policies that require the use of one link instead of another. This mode is useful when the enterprise needs to send the Web traffic to a broadband link.

In parallel to defining a strategy to select the best path, an enterprise is required to follow some additional configuration steps for adding WAN Security. In the figure, notice that as the Ipanema appliance is installed before the Internet router, IPsec NAT traversal is required to detect and establish the tunnels. For instance, configuring Internet access requires the user to:



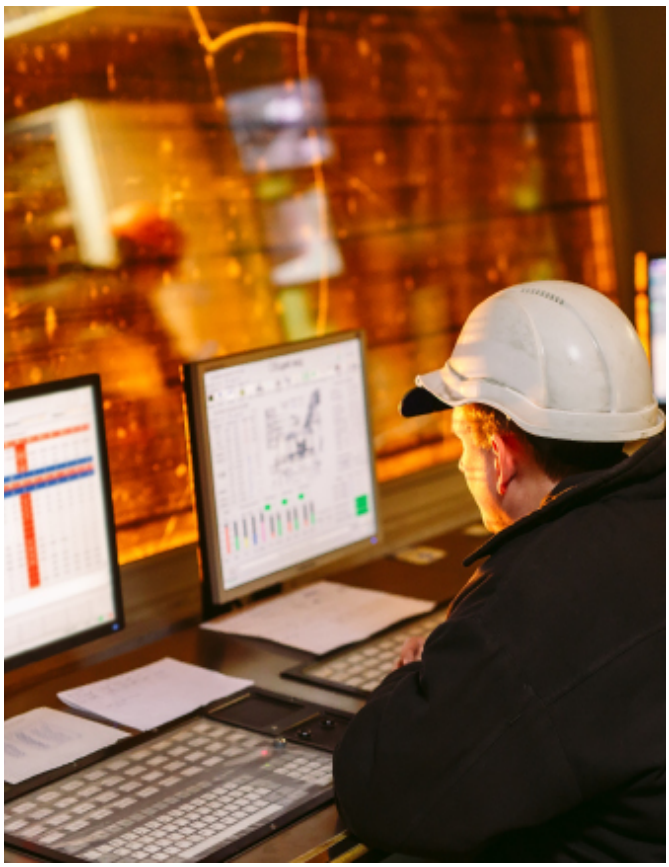
1. Activate IPsec concentrators in the datacenter which includes the IP address encryption and authentication parameters of the concentrator to which the branch will be connected.

2. Activate direct-to-Internet exceptions, defining the traffic that will be tunneled to Secure Web Gateways (by default, outbound HTTP/HTTPS are not tunneled), through user-generated rules that account for protocols, subnets or L4 ports.

3. Add Secure Web gateways, by defining primary and secondary gateways, including IP addresses.

4. Create the Internet access links, from the available WAN links in the branch appliances.

5. Set the Internet access parameters, by associating the preconfigured IPsec concentrators, Internet access, Secure Web gateways and security exceptions.



Benefits

For the enterprise as a whole: DWS and WAN Security (i.e. Hybrid WAN) accelerate the adoption of "on-premise" collaborative and SaaS applications (e.g. Skype for Business, Office 365, G Suite) by deploying abundant bandwidth through secure and high-performing hybrid WAN. Increase SaaS application performance from the cloud by using peering points (e.g. Equinix) of specific SaaS applications. To further improve business continuity for all applications even in the case of a single link and/or single appliance failure, the Dynamic WAN Selection and WAN Security features (i.e. DWS + WAN Security = Hybrid WAN) can be made redundant thanks to the High Availability (HA) feature. HA clusters (pair of Ipanema appliances working in active/standby mode) secure the availability of the Hybrid WAN feature to ensure a site is always connected to any available WAN.

For the IT organization: Simplify hybrid WAN deployments by activating WAN Security without additional specialized appliances. Simplify IT management by eliminating the configuration of additional firewalls in the branch offices. Easily configure end-to-end secure local-break-out(s), through Secure Web gateways.

For the end user: Increase end-user productivity while preserving confidentiality and security. Take advance of fast Web browsing and fast and secure access to the Cloud and SaaS applications, in remote international locations.

KEY DIFFERENTIATORS TO REMEMBER

- **Simplify Hybrid WAN deployments:** Ipanema appliances allow you to protect your branch Internet connections from threats, without using additional security devices.
- **Full-integrated with performance and visibility:** WAN Security cooperates with DWS and the Application Control and Application Visibility features, as part of an integrated, autonomic system.
- **Friendly Secure Web Gateways integration:** Streamline the implementation of local-break-out(s).
- **Accelerate the adoption of "on-premises" collaborative and SaaS applications:** By having abundant bandwidth through secure and optimal hybrid WAN.

About Infovista

Infovista, the leader in modern network performance, provides complete visibility and unprecedented control to deliver brilliant experiences and maximum value with your network and applications. At the core of our approach are data and analytics, to give you real-time insights and make critical business decisions. Infovista offers a comprehensive line of solutions from radio network to enterprise to device throughout the lifecycle of your network. No other provider has this completeness of vision. Network operators worldwide depend on Infovista to deliver on the potential of their networks and applications to exceed user expectations every day. Know your network with Infovista.

KNOW YOUR NETWORK™