Pulse Secure®

Asia-Pacific SSL VPN

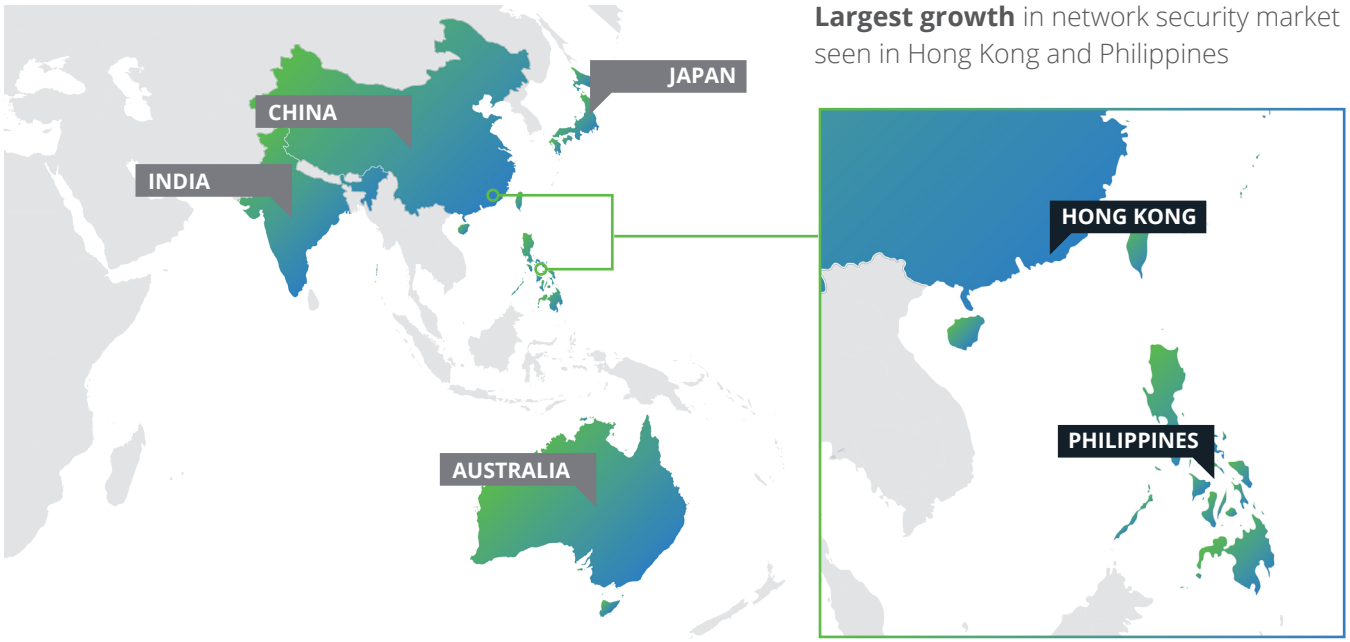
Mobile and Cloud Continue to Drive SSL VPN Growth

Table of Contents

Market Trends

The Asia-Pacific network security market is growing at an impressive 17.5% YoY. The network security market includes firewall, IDP/IPS, and SSL VPN. The largest area of growth is SSL VPN with 24.6%. The Asia-Pacific network security market is growing at a faster pace than the 7.8% growth rate of the global network security market.

The strongest performance in Asia-Pacific is seen in China, Japan, Australia, and India with the largest growth happening in the Philippines and Hong Kong. Cyber Attacks are driving governments to create initiatives and service providers to offer robust security solutions.



Largest growth in network security market seen in Hong Kong and Philippines

ASIA-PACIFIC NETWORK SECURITY MARKET GROWTH YoY

17.5%

LARGEST AREA OF GROWTH IS

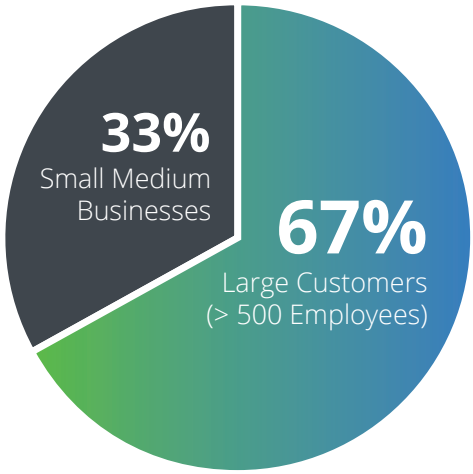
SSL VPN 24.6%

The growth in cyber-attacks has led to government initiatives that require organizations to increase their threat prevention and minimize threat surfaces. Given the business impacts (reputation and profitability), Chief Information Security Officers (CISOs) are seeing more budget allocated to keeping the organization safe and raising internal awareness.

Managed Security Service Providers (MSSPs) are also offering more robust services to those customers whose IT teams cannot keep up with growing security requirements. Service Providers (SPs) are not only investing in order to manage traffic growth but also to increase added service offerings with enhanced security.

For the enterprise customers in this market, large customers (> 500 employees) make up 67% of the business, while SMB make up the other 33%.

It is very clear that the network security market is growing rapidly and SSL VPN continues to be a catalyst of that growth.



Purpose-built SSL VPN vs. Add-Ons to Other Technology

Integrated Security Appliances (ISA) and Unified Threat Management (UTM) devices make sense in theory. Imagine this: a single appliance which can handle more than one of the security needs of an organization while also being easy to manage, an ideal situation for any company. The pricing of additional add-ons after the initial purchase may also seem like an attractive proposition. However, actual deployments tell a more complex and compromising story, which in the long run end up costing more. These compromises come in the form of performance or feature hits.

Performance is directly affected as you turn on functionality. For example, a next-generation firewall can see **traffic drop to 30%** of marketed performance simply by turning on SSL inspection. Vendors react by telling customers to deploy appliances with only one function deployed. In regards to feature compromises, most integrated appliances have SSL VPN as an add-on while accepting "good enough" functionality. This limits the type of connection options available, such as being limited to Layer 3 client connections only. Other feature limits can include minimal application support and functionality. With these limits, multiple gateways need to be deployed to cover all of the use cases and connectivity options.

Conversely, a dedicated **SSL VPN appliance ensures that 100% of resources** are focused on the SSL traffic. These purpose-built appliances provide the broadest set of SSL VPN features with the richest set of functionality and application support. Dedicated SSL VPN appliances may provide a single point of entry to a network regardless of device type access (mobile, desktop, and IoT), the access method (client, clientless, and SDK) or destination (Internal servers, data stores, VDI servers, or cloud apps).

Cloud Migration

The migration from on-premise or datacenter deployments to cloud is a misunderstood trend when it relates to SSL VPN. Some companies who are deploying cloud infrastructure think that SSL VPN is irrelevant. Yet, the reality is that most enterprises are phasing their migration to the cloud, which has been defined by the Hybrid IT infrastructure. Also, organizations are considering how they can move to the cloud without compromising on their security policy.

Migrating applications and data to the cloud does not have to mean losing visibility into the device state or losing track of what applications are being accessed. One can extend their existing SSL VPN investment by enforcing the same security policy when their users access on-premise and/or cloud-based data and services. SAML-enabled SSL VPN offerings can also provide Single Sign-On (SSO) and enhance the end-user experience that provides many aspects of Identity Access and Management (IAM) offerings.

Growth in Mobile

The growing demand of enterprise mobility has also increased SSL VPN demand. As employees demand productivity access via their smartphones, more employers are embracing Bring Your Own Device (BYOD). This means more access across more device types. However, the experience of using smartphones has set a new access status quo expectation, where all VPN experiences should be simple and transparent. This can be achieved by using combination of location awareness, certificate-based authentication, and per-application VPN.

Another aspect of SSL VPN to consider for mobile BYOD is provisioning. While organizations want to allow BYOD, the cost of provisioning and support of these devices is a concern. An SSL VPN offering that provides an efficient way to provision or onboard devices becomes attractive, while accelerating the adoption of BYOD.

Why Pulse Connect Secure?

Better End-User Experience

Connect Secure's feature-rich VPN solution is centered around delivering an optimal end-user experience, enabling the productivity needs of the next-generation worker. Access to mobile and cloud resources are securely available to your workforce on the go. Pulse Connect Secure's user-centric features eliminate the kludgy and invasive traits that were associated with remote access solutions of the past. For those that want to make the deployment completely transparent for their end users, certificate-based authentication, smart connection management, and single sign-on (with or without SAML) are available. The end-user can just use their apps and software their personal way without any new training or extra steps.

As consumerization of IT from BYOD to Cloud continues to grow, having SAML 2.0 in both Service Provider (SP) and Identity Provider (IdP) is important.

Most deployments when using Cloud Apps will be available when the VPN device is an IdP. The lack of this support adds another layer of complexity for the end-user, where they will need to relearn how to connect to an app. With Pulse Connect Secure, the capability of SAML 2.0 in both SP and IdP mode, end users now go to the apps they want to use, just as they naturally do.

Better Admin Experience

With the recent IT transformations, Pulse Secure is supporting the role of IT as it evolves from gatekeeper to enabler. For the administrator, simple configuration and deployment options are essential. For configuration, the interface that supports Connect Secure is purely web-based, no longer requiring an additional application. The recent release not only delivers simplicity but also flexibility. The comprehensive dashboards and reports give the administrator the mission-critical information needed for network health and performance. Additional features like Policy Tracing help the administrator easily determine what is happening with certain connections. Configuration management for a global or national deployment is even further simplified when using Pulse One, a newly released centralized management solution.

Flexible Deployment Options

Pulse Secure believes a single device should be able to handle all the connection scenarios. Not only is this beneficial for the admin, but also for the end user. A single access point, vpn.company.com, regardless of device or location makes it easy for end users. Knowing that one can use any device and any browser means less calls to IT and connection challenges.

With Role Based Access Control, employees, contractors, guests, and so on can only get access to the resources that are defined within their roles. Defining access policies is based on a combination of variables such as user, group, location, and device compliance state.

Connect Secure is also available on physical and virtual appliances, allowing for more deployment flexibility.

Built for the Future

Optimal and Secure Browser Experience Connect Secure has moved away from Java, Silverlight, ActiveX, and other browser technologies that are historically renowned for their compatibility and security challenges. Most browsers have disabled these, yet other vendors continue to leverage these technologies, while delivering a painful and insecure end user experience.

On the other hand, Connect Secure supports HTML5 with WebSockets. Along with the built-in HTML5 to RDP/Telnet/SSH broker – remote access has never been easier and more compatible. Zero applets or plug-ins are needed. Device agnostic RDP sessions set up in seconds. Competing vendors have limited support here and do not have a built-in HTML5 broker, as they recommend you go to other companies and try to deploy something separately on other hardware.

Cloud Secure is a new capability that enables user authentication, device compliance checks, and access to all apps, either on-premise or in the cloud. This optimizes the end user experience while giving IT the comprehensive visibility and control for a hybrid IT environment. With other VPN vendors, you would need to purchase other products to achieve a limited solution benefits.

Authentication Servers and Multi-factor Authentication (MFA) Over the years, we've added support for majority of the single and multi-factor authentication vendors. Support and documentation is available to help you integrate with any authorization server of your choice.

Onboarding and Provisioning Easily push clients, VPN profiles, WiFi profiles, and certificates to end devices (both desktops and mobile) using our automated, self-service portal. This frees IT from the burden of configuring corporate or BYOD devices. Others may not provide remote onboarding or device provisioning.

Market Leading Rewriter With its core history of SSL VPN, Pulse Secure continues to provide the best portal and rewriter experience to support the broadest applications, extending the out-of-the-box experience. Other solutions need additional resources to customize and modify a sub-optimal experience with limited features, resulting in a poor end user acceptance. At Pulse Secure, this is not an issue making it clear why analysts and customers trust us with their business needs.

How PCS Ties in to the Full Secure Access Story

Connect Secure is the foundation of Pulse Secure's Secure Access Suite. The Secure Access Suite is an all-in-one solution that enables mobile access to the data center, extends security compliance to the cloud, and provides complete visibility of your corporate network.

About Pulse Secure, LLC

Pulse Secure, LLC is a leading provider of secure access solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize the company's virtual private network (VPN), network access control (NAC) and mobile security products to enable end-user mobility securely and seamlessly in their organizations. Pulse Secure was formed in 2014 from Juniper Networks' Junos Pulse business. Pulse Secure's mission is to deliver secure access solutions for people, devices, things, and services.

www.pulsesecure.net