silver peak™

Increasing Cloud Application Performance With Secure Internet Breakout

First-packet iQ and Cloud Intelligence Enable Granular Security Policy Enforcement

Cloud Adoption Continues to Accelerate

Enterprises continue to move applications to the cloud. Knowledge workers now regularly use Software as-a-Service (SaaS) applications such as Office365, Salesforce and Workday, access email from cloud-hosted services, store documents and backups on Box, Dropbox or the like. ERP and CRM systems are primarily cloud-hosted today. Enterprises increasingly choose Infrastructure as-a-Service (IaaS) solutions for lower costs while increasing IT agility. In fact, IDC estimates that 78% of all workloads will be processed in public or private cloud data centers by 2018*.

However, workers in branch offices commonly complain that cloud-hosted applications perform better from home than from the branch. Why? Because from home, SaaS application and IaaS access is directly over the internet at speeds of up to 100Mbps or even higher. With the traditional router-centric branch WAN edge model, access is not direct to the internet. All internet-bound traffic is backhauled to a headquarters or hub site where additional security screening is performed to protect the enterprise from vulnerabilities. Basic SD-WAN solutions also employ an "all-or-nothing" approach to handling internet-bound traffic or must rely on a manual process for configuring Access Control Lists (ACL) on every appliance to identify specific IP addresses to steer trusted SaaS applications directly to the internet. Not only is traffic backhaul inefficient – potentially requiring additional and costly bandwidth – it also adds latency which negatively impacts cloud application performance resulting in decreased worker productivity and satisfaction. Additionally, SaaS address ACLs become obsolete within days requiring another round of manual programming.

*IDC FutureScape: Worldwide Cloud 2016 Predictions, https://www.idc.com/promo/thirdplatform/RESOURCES/ATTACHMENTS/IDCFutureScapeExec-Summary-Cloud.pdf

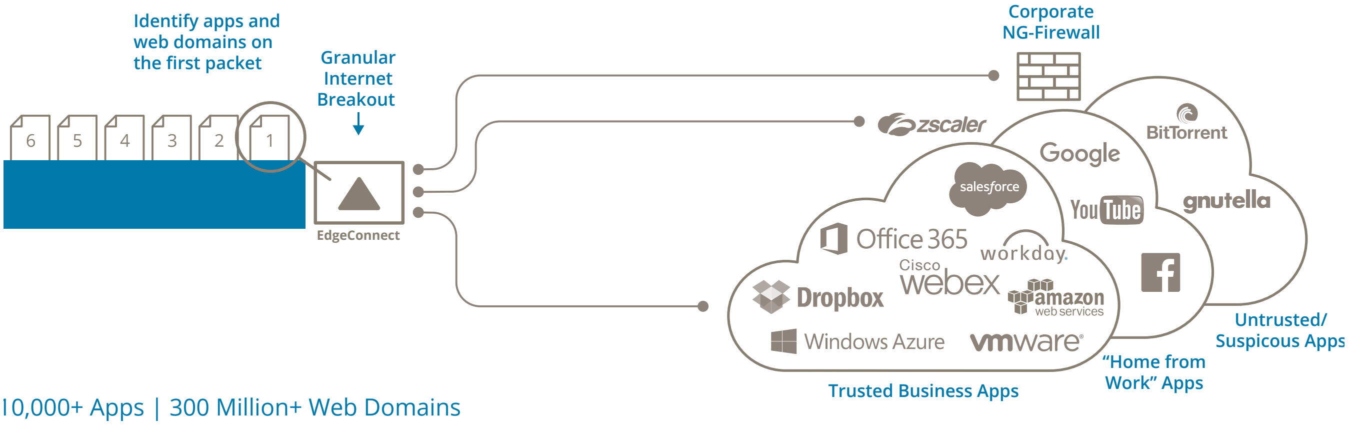


Figure 1: Granular traffic steering requires application classification on the first packet.

Use Case: Secure Internet Breakout

Direct access to cloud applications from the branch over the internet delivers the highest performance. But not all applications are equal, and some web traffic can expose the enterprise to viruses, trojans, DDoS attacks and other vulnerabilities. Therefore, direct cloud breakout must also be secure.

The challenge that the SD-WAN must meet is the ability to granularly steer internet-bound HTTP and HTTPS traffic on an application-by-application basis to the correct destination based on corporate security policies, see Figure 1. For example, a security policy might be defined as follows:

- Send all known, trusted business SaaS traffic such as Office365, Salesforce, Workday and Box directly to the internet
- Send "home from work" recreational applications like Facebook, Twitter, YouTube and Netflix to a secure web gateway service such as Zscaler
- Send all untrusted, suspicious and unknown traffic such as peer-to-peer traffic or traffic to countries in which the company does not do business back to a hub or headquarters-based next-generation firewall from Palo Alto, Fortinet or Check Point

Implementing a granular security policy for web applications requires granular traffic steering since many HTTP and HTTPS applications share the same TCP ports. However, the steering decision must be made on the first packet of the application. Once an application session – or flow – has been established, it cannot be moved to an alternate path.

There are two challenges to granularly steer traffic on the first packet and therefore two required capabilities:

- Ability to identify applications on the very first packet to steer traffic to the correct destination
- Maintaining an up-to-date SaaS application IP address database – or "map of the internet" – resident in SD-WAN appliances since these addresses change continously

Challenge #1: First-packet Application Identification

Traditional application classification techniques utilize a combination of well-known IP addresses, TCP/UDP port numbers and Deep Packet Inspection (DPI). DPI is useful when applications use ports unpredictably, or when you must distinguish applications that share the same HTTP or HTTPS port. However, DPI is not sufficient to granulary steer traffic to a specific destination based on the application because it cannot identify the application on the first packet. DPI relies on a library of application signatures and heuristics, requiring two to six packets to identify an HTTP application and 10 packets or more to identify an HTTPS application. While this is acceptable for flow reporting, QoS marking and even blocking a connection, it is unable to support granular traffic steering required to implement fine-grained security policies across the WAN.

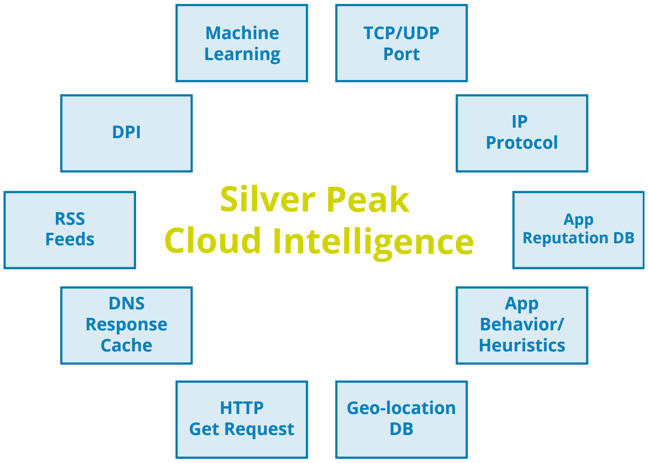


Figure 2: First-packet iQ employs multiple techniques to classify more than 10,000 SaaS and web applications and 300 million web domains.

The Railroad Analogy

Imagine several trains that consist of an engine and multiple boxcars traveling from San Francisco. Trains carrying furniture need to be directed east to Denver, and trains carrying aerospace components need to be directed south to Los Angeles. However, you are not able to determine the cargo that the train is carrying until the engine and three to five boxcars have passed the railroad switch.

The engine represents the first packet of a TCP/IP flow and the boxcars represent subsequent packets of the flow. As the train approaches the switch to connect to the different tracks serving Denver and Los Angeles, the switch operator can't wait until the fifth, third or even the second boxcar has passed. To avoid a disastrous outcome, the routing decision for the train must be made before the engine reaches the switch. Therefore, a technique is required to identify the boxcar contents before the engine passes the switch.

Solution: First-packet iQ Application Classification

To steer traffic to its correct path in order to enforce security policies, traffic must be classified on the very first packet of a flow. Silver Peak Unity EdgeConnect First-packet iQ identifies more than 10,000 applications and more than 300 million web domains on the first packet. First-packet iQ goes beyond typical DPI and port-level approaches used today and adds Cloud Intelligence to maintain an up-to-date database of IP addresses used by SaaS applications.

First-packet iQ employs multiple techniques as shown in Figure 2 to classify applications providing unprecedented application visibility and a superior identification confidence level.

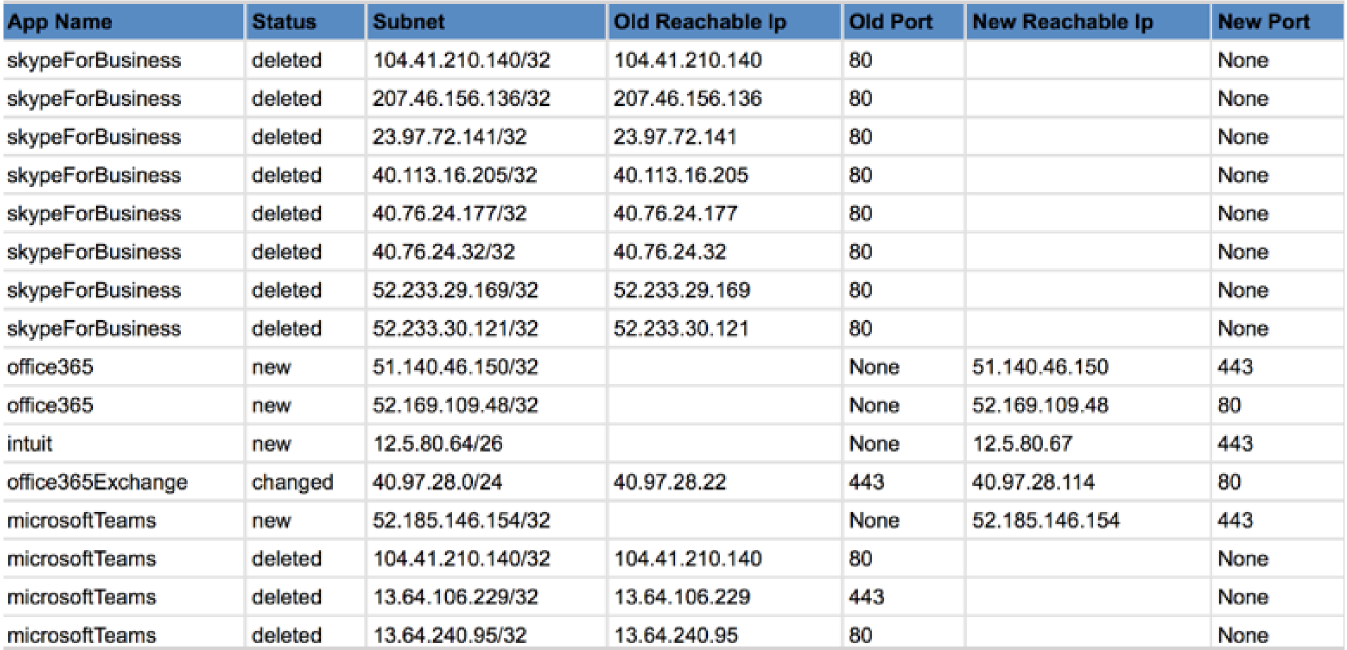
Challenge #2: SaaS IP Addresses Change Every Day

Popular, highly-subscribed SaaS applications such as Office365, Salesforce, Workday, Box, Dropbox, and others employ hundreds or even thousands of IP addresses to support their huge number of users. These IP addresses are not static; they may be re-allocated to a different region or to a different application. New addresses are added frequently to keep up with end user demand. In short, the pool of IP addresses used by SaaS applications changes almost continuously. Table 1 is a short excerpt from a daily SaaS application subnet change report showing addresses deleted and those added to the IP address pool for Skype for Business and Office365.

Some SD-WAN solutions claim to steer applications on the first packet, and they can accomplish this using ACLs. However, ACLs are static and must be manually programmed. A security policy may work properly when initially configured but fail days or weeks later after SaaS application IP addresses change. Manual re-programming of IP addresses into ACLs simply cannot stay current with the dynamic nature of SaaS applications.

Solution: Cloud Intelligence to Keep Pace With Continuously Changing SaaS IP Addresses

Silver Peak Cloud Intelligence maintains a centralized application database or “map of the internet” that is continuously updated based on the application classification techniques described previously. On a daily basis, EdgeConnect SD-WAN appliances receive



App Name	Status	Subnet	Old Reachable Ip	Old Port	New Reachable Ip	New Port
skypeForBusiness	deleted	104.41.210.140/32	104.41.210.140	80		None
skypeForBusiness	deleted	207.46.156.136/32	207.46.156.136	80		None
skypeForBusiness	deleted	23.97.72.141/32	23.97.72.141	80		None
skypeForBusiness	deleted	40.113.16.205/32	40.113.16.205	80		None
skypeForBusiness	deleted	40.76.24.177/32	40.76.24.177	80		None
skypeForBusiness	deleted	40.76.24.32/32	40.76.24.32	80		None
skypeForBusiness	deleted	52.233.29.169/32	52.233.29.169	80		None
skypeForBusiness	deleted	52.233.30.121/32	52.233.30.121	80		None
office365	new	51.140.46.150/32		None	51.140.46.150	443
office365	new	52.169.109.48/32		None	52.169.109.48	80
intuit	new	12.5.80.64/26		None	12.5.80.67	443
office365Exchange	changed	40.97.28.0/24	40.97.28.22	443	40.97.28.114	80
microsoftTeams	new	52.185.146.154/32		None	52.185.146.154	443
microsoftTeams	deleted	104.41.210.140/32	104.41.210.140	80		None
microsoftTeams	deleted	13.64.106.229/32	13.64.106.229	443		None
microsoftTeams	deleted	13.64.240.95/32	13.64.240.95	80		None

Table 1: Daily IP address changes such as those seen here for Office365 and Skype-for-Business require an internet map that is continuously updated.

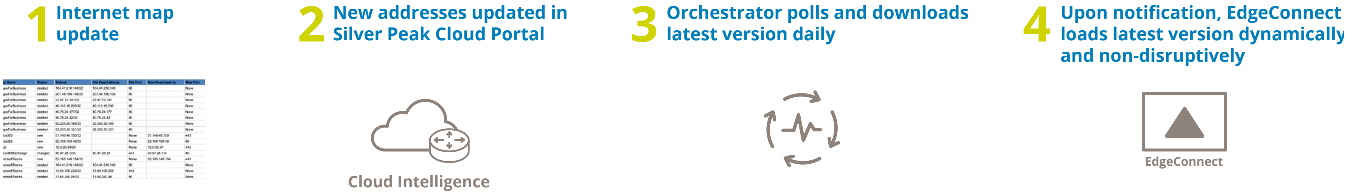
an update to their resident application address database to remain current with changing SaaS and web IP addresses, as shown in Figure 3. This update process is similar to that employed by a computer virus protection application.

Integrated Zone-based Stateful Firewall

An integrated zone-based stateful firewall is essential for a complete, secure cloud breakout solution enabling direct internet connectivity to trusted SaaS applications and IaaS from branch offices. The EdgeConnect zone-based firewall further hardens the enterprise WAN by blocking unwanted or unauthorized traffic attempting to enter the branch network. The only inbound sessions allowed are responses to communications initiated from within the branch or to ports whitelisted and opened up for trusted inbound communication, for example, to remotely manage a printer or teleconferencing system.

Simple, Centralized Security Policy Administration and Automated Updates

A key benefit of a complete SD-WAN solution is simplified, centralized orchestration. Through an intuitive graphical user interface (GUI), Silver Peak Unity Orchestrator streamlines configuration and distribution of security policies to all appliances in the EdgeConnect SD-WAN fabric. This results not only in significant operational cost savings but also reduces the potential for incorrect application handling due to human error. Orchestrator uses industry-standard application groupings by traffic type such as email, voice and video and by content type such as auctions, automotive, aviation, education, fantasy sports, social media and more (Figure 4) to further simplify security policy definition. As described previously, automated daily updates of the application IP address database to EdgeConnect appliances keep pace with SaaS and web address changes.



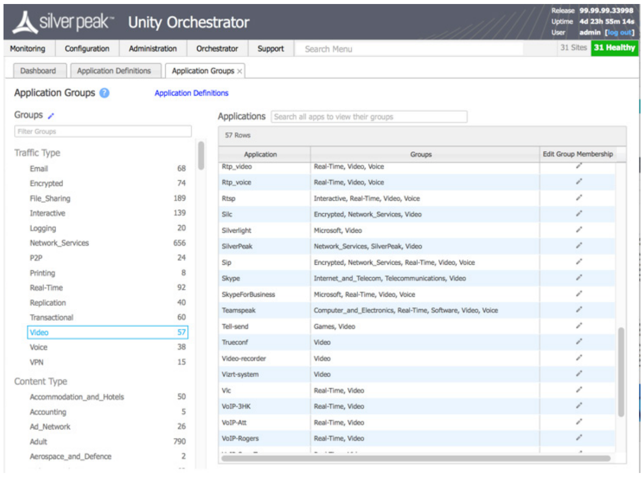
1 Internet map update

2 New addresses updated in Silver Peak Cloud Portal

3 Orchestrator polls and downloads latest version daily

4 Upon notification, EdgeConnect loads latest version dynamically and non-disruptively

Figure 3: Application IP address database is updated daily to every EdgeConnect appliance.



Traffic Type	
Email	68
Encrypted	74
File_Sharing	189
Interactive	139
Logging	20
Network_Services	656
P2P	24
Printing	8
Real-Time	92
Replication	40
Transactional	60
Video	57
Voice	38
VPN	15
Content Type	
Accommodation_and_Hotels	50
Accounting	5
Ad_Network	26
Adult	790
Aerospace_and_Defence	2

Application	Groups	Edit Group Membership
Rtp_video	Real-Time, Video, Voice	✎
Rtp_voice	Real-Time, Video, Voice	✎
Rtsp	Interactive, Real-Time, Video, Voice	✎
Silc	Encrypted, Network_Services, Video	✎
Silverlight	Microsoft, Video	✎
SilverPeak	Network_Services, SilverPeak, Video	✎
Sip	Encrypted, Network_Services, Real-Time, Video, Voice	✎
Skype	Internet_and_Telecom, Telecommunications, Video	✎
SkypeForBusiness	Microsoft, Real-Time, Video, Voice	✎
Teamspeak	Computer_and_Electronics, Real-Time, Software, Video, Voice	✎
Tell-send	Games, Video	✎
Trueconf	Video	✎
Video-recorder	Video	✎
Vizrt-system	Video	✎
Vlc	Real-Time, Video	✎
VoIP-3HK	Real-Time, Video	✎
VoIP-Att	Real-Time, Video	✎
VoIP-Rogers	Real-Time, Video	✎

Figure 4: Application grouping simplifies security policy administration.

Optimal Egress Routing for Backhauled Traffic

Direct internet breakout from the branch provides the highest SaaS application and IaaS performance. However, for sites not served by internet connections or if corporate security policies require backhaul of SaaS applications for additional security screening, Silver Peak Cloud Intelligence includes information to optimally route traffic for the best performance. The Silver Peak SaaS optimization feature measures the loss, latency and other metrics from EdgeConnect devices to physical egress points where SaaS providers' data is being served. This information is updated continuously to appliances in the EdgeConnect SD-WAN providing the optimal end-to-end path for any user to the SaaS application.

Business Outcomes

As enterprises continue their migration to the cloud, they increasingly adopt a "cloud-first" SD-WAN architecture to provide the highest levels of SaaS application and IaaS performance providing a number of tangible business benefits to the enterprise. The Silver Peak EdgeConnect SD-WAN solution with First-packet iQ and Cloud Intelligence delivers the highest performance for the cloud-first enterprise while protecting branch offices from unwanted threats and vulnerabilities.

EdgeConnect Solution Benefits	Business Outcomes
Increased SaaS application and IaaS performance and availability	Increase employee and business productivity
Predictable SaaS application performance	Enhance customer satisfaction
Granular application-driven security policies enabled by First-packet iQ	Reduce security risks
Automated SaaS IP address tables and internet map updates	Increase operational efficiency and mitigate human error
Integrated zone-based stateful firewall	Reduce security risks

Table 2: Silver Peak Unity EdgeConnect SD-WAN solution delivers tangible benefits and business outcomes.

Company Address

Silver Peak Systems, Inc
2860 De La Cruz Blvd.
Santa Clara, CA 95050

Phone & Fax

Phone: +1 888 598 7325
Local: +1 408 935 1800

Online

Email: info@silver-peak.com
Website: www.silver-peak.com