SOLUTION BRIEF

CLOUD ACCESS PROXY – OPTIMIZING AND SECURING SAAS DEPLOYMENTS

ENSURE SECURE ACCESS TO YOUR SAAS APPLICATIONS WHILE IMPROVING PERFORMANCE AND USER EXPERIENCE

Traditionally, enterprise networks were designed to provide users with access to applications and services hosted locally, within their data centers. Office productivity and storage applications were accessed through east-west flow of the traffic within the network. To secure user access to the internet and to protect them from cyberthreats, a large central security stack was typically hosted to inspect traffic going in and out of the network.

ENTERPRISE NETWORKS ARE RAPIDLY CHANGING

As organizations grew and expanded into multiple branch offices, they were forced into a hub-and-spoke deployment model where all branch office traffic was routed back to the central security stack for policy enforcement and inspection. This deployment model worked well enough in legacy enterprise networks and the latency introduced by traffic backhauling did not impact user experience.

However, with the increased adoption of SaaS-based applications, as well as the rapid move towards multi-cloud deployments, enterprise networks are rapidly changing. According to a recent report, 60 percent of enterprises are already using some form of SaaS in their day-to-day operations.[1] Legacy productivity software like Microsoft Office applications are rapidly being moved to the cloud and being replaced by Microsoft Office 365. Similarly, cloud versions of storage applications like Dropbox are proliferating. Cisco also reports that by the year 2021, 94 percent of workloads will be processed by cloud-based data centers.[2]

CHALLENGE

- Traditional enterprise networks are not optimized for SaaS traffic
- Security provided by SaaS providers is not enough
- Lack of visibility can cause data loss and insider abuse

SOLUTION

- Local breakout helps optimize SaaS traffic
- Tenant access control helps stop data loss
- Full visibility into sanctioned and unsanctioned SaaS traffic

BENEFITS

- Optimize traffic flow and network performance
- Enhance user experience
- Ensure data protection between sanctioned and unsanctioned SaaS
- Improve TCO

[1] https://www.computereconomics.com/article.cfm?id=2253

[2] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html

LEGACY SECURITY STACKS DO NOT SCALE WELL WITH SAAS

Legacy proxies and security solutions are neither designed nor optimized for highly demanding cloud applications. And productivity software like Office 365 presents a unique challenge in that each individual user creates dozens of long-lived connections to the cloud. However, even though documents are now accessed frequently from the cloud and edited online instead of locally, the user experience is still expected to be the same.

With a hub-and-spoke security model, all branch office traffic, including SaaS traffic, is backhauled to the corporate security stack before being sent to the internet. A significant strain is put on the security stack, which was neither designed nor sized to cope with such high-performance demands. This creates performance bottlenecks and introduces network latency, which severely degrades the user experience.

To alleviate these problems, SaaS providers recommend enterprises to identify SaaS traffic close to the source, bypassing the central security stack, and routing it directly to the cloud. This ensures optimal performance and user experience, but at the cost of visibility to the central security stack.

Such deployments, coupled with a lack of visibility, can create major security problems. Large enterprises on an average use around 1,200 cloud services, including sanctioned and unsanctioned applications. According to Cisco, almost 98 percent of these are shadow IT.[3] Without visibility into sanctioned and unsanctioned application traffic, organizations cannot maintain fool-proof security in their networks spotting anomalies and security incidents instantly.

In addition, enterprises are increasingly opting for SD-WAN solutions, which removes WAN links using expensive MPLS circuits, and replaces them with broadband connections. However, these solutions lack security features necessary to protect SaaS data and users from threats. At the same time, these solutions are always undergoing changes to try and adapt to the rapidly changing market. This can essentially lock users down with an inferior solution without a choice to change.

A10 NETWORKS CLOUD ACCESS PROXY (CAP) SOLUTION

A10 Networks' Cloud Access Proxy (CAP) is a complete solution, designed specifically to help organizations optimize the performance and security of their SaaS application traffic.

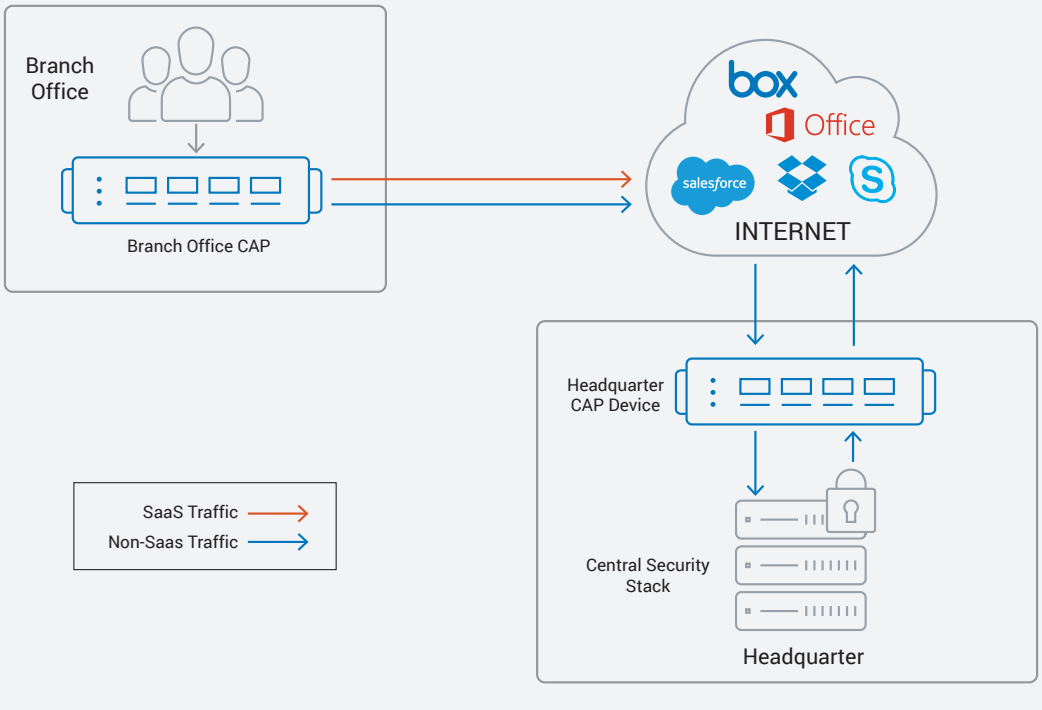

Figure 1: CAP optimizes SaaS traffic flow by performing local breakout at the branch office

[3] https://blogs.cisco.com/cloud/gartner-report-says-shadow-it-will-result-in-13-of-security-breaches

The CAP solution is divided into three main parts:

BRANCH OFFICE

This small branch office device is designed to identify and separate SaaS traffic from non-SaaS traffic right at the source. Once this "local breakout" is performed, the SaaS traffic is routed to the cloud, bypassing the central security stack at the headquarters while all other traffic is backhauled for inspection. This device can also be used to filter traffic at the branch office and restrict user access for added security. Tenant access control can also be performed here, ensuring no data loss occurs due to unsanctioned tenants.

CENTRAL/HEADQUARTERS DEVICE

The central/headquarters device contains all the features available in the branch office CAP, but it can perform at a higher scale, ensuring no bottlenecks are created at the headquarters, where the central security stack resides. This device also augments the central security stack to ensure security policies are enforced and traffic is inspected at optimal performance.

CENTRALIZED VISIBILITY

With centralized visibility users can gain full visibility into SaaS and non-SaaS traffic and gain actionable insights from all branch offices, the headquarters and the cloud at a centralized location. This enables users to address any concerns they might have related to Shadow IT, be informed about any abnormal activity spikes or security events that might occur anywhere in their network.

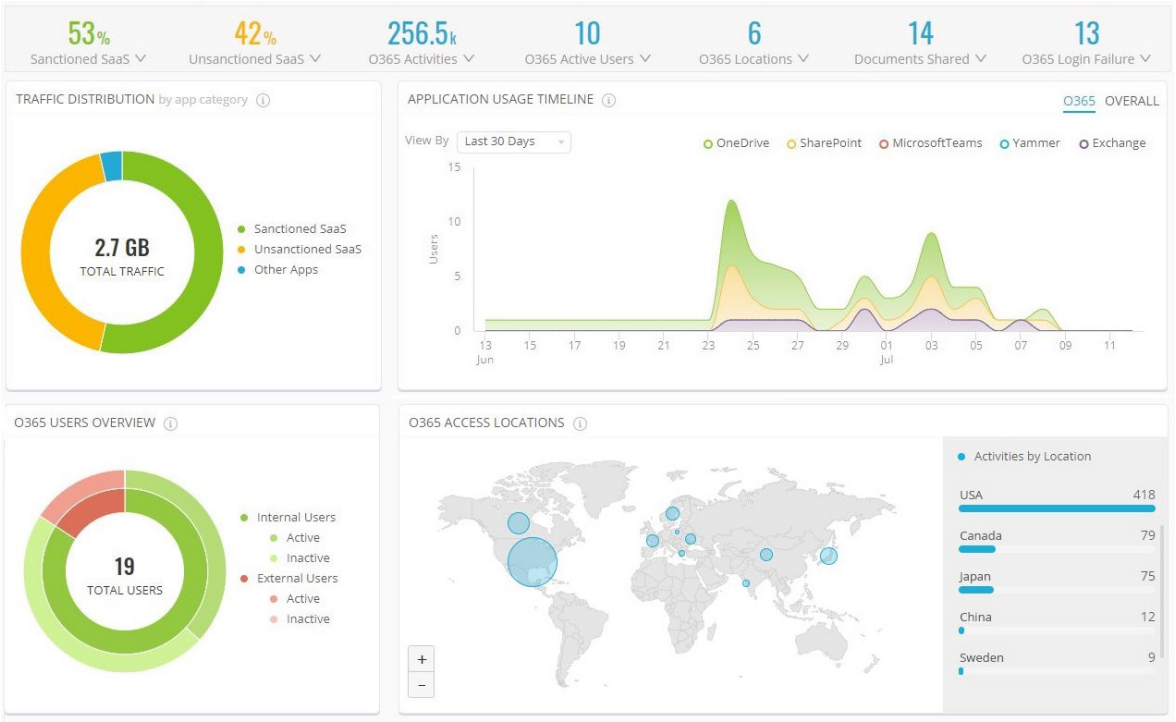

Figure 2: Centralized visibility into traffic from all branch offices, the headquarters and the cloud, ensures no security events are missed

SUBSCRIPTION-BASED MODEL

The CAP solution is available with a term-based subscription bundle that includes a number of Branch Office CAP, Central/ Headquarters devices and the CAP Visibility & Analytics solution for centralized management and visibility. Enterprises can buy 1-, 3- or 5-year bundles based on number of users on their network. This OPEX budgeting model helps organizations avoid being locked in with a vendor and helps them improve their TCO significantly.

FEATURES AND BENEFITS

The A10 Networks CAP solution enables enterprises to:

- Optimize branch office network performance and enhance user experience by performing local breakout, routing SaaS traffic directly to the cloud, while backhauling non-SaaS traffic to the central security stack for inspection.
- Dynamically distribute traffic across multiple WAN links using Next Hop Load Distribution (NHLD).
- Prevent data theft by enforcing tenant access control, allowing only sanctioned tenant accounts to be accessed throughout the enterprise.
- Gain application level visibility and control, with per-application policy management.
- Protect users from external threats by filtering out traffic based on URL and SNI information.
- Secure internet traffic that is backhauled from branches to the central security stack using IPsec VPN tunnels.
- Protect enterprise users and resources from incoming attacks with the stateful firewall.
- Deploy the branch office CPE, quickly and with ease, using the one-step configuration wizard.
- Gain centralized visibility into traffic from all branch offices, the headquarters and the cloud, ensuring no security events are missed.
- Gain visibility into Shadow IT and unsanctioned SaaS usage for additional security.
- Customize dashboards by adding/removing widgets according to your specific needs.
- Improve TCO with the subscription bundle offering for greater operational flexibility.

SOLUTION COMPONENTS

The A10 Networks CAP solution is made up of the following components:

- Thunder 840 CAP for small branch offices
- Thunder 1040, Thunder 3040 or any Thunder CFW appliance for large branch offices or headquarters
- Cloud Access Proxy Visibility & Analytics solution for centralized visibility
- A10 URL classification service for traffic filtering and bypassing
- A10 application visibility and control service

CLOUD ACCESS PROXY VISIBILITY AND ANALYTICS SPECS

	VIRTUAL	BARE METAL
Supported Hypervisors	VMware ESXi 5.5 and 6.5	N/A
Minimum Hardware Requirements	• Intel x86-based CPUs with minimum of 16 cores • 32 GB RAM • 220 GB of free disk space	• Intel x86-based CPUs with minimum of 16 cores • 32 GB RAM • 220 GB of free disk space

CLOUD ACCESS PROXY HARDWARE APPLIANCES SPECS

PERFORMANCE	THUNDER 840 CAP	THUNDER 1040 CFW	THUNDER 3040 CFW
Throughput	0.5 Gbps	20 Gbps	30 Gbps
Application CPS	5K	180K	280K
Concurrent Sessions	4 Million	32 Million	64 Million
SSL INSIGHT PERFORMANCE*1			
SSLi Throughput	N/A	1.5 Gbps	2.5 Gbps
SSLi CPS		RSA: 4K ECDHE: 3K	RSA: 8K ECDHE: 4.5K
NETWORK INTERFACE			
1 GE Copper	5	5	6
1 GE Fiber (SFP)	0	0	2
1/10 GE Fiber (SFP+)	0	4*5	4
Management Ports	1 x Ethernet Mgmt port, 1 x RJ-45 console port		
HARDWARE SPECIFICATIONS			
Processor	Intel Communications Processor	Intel Communications Processor	Intel Xeon 4-core
Memory (ECC RAM)	8 GB	8 GB / 16 GB*2	16 GB
Storage	SSD	SSD	SSD
Hardware Acceleration	Software	Software	Software
Switching/Routing	Software	N/A	Software
SSL Security Processor ('S' Models)	N/A	Yes	Yes
Dimensions (inches)	1.75 (H) x 17.0 (W) x 12 (D)	1.75 (H) x 17.5 (W) x 17.25 (D)	1.75 (H) x 17.5 (W) x 17.45 (D)
Rack Units (Mountable)	1U	1U	1U
Unit Weight	8.8 lbs	15 lbs 17 lbs (RPS)	20.6 lbs
Power Supply (DC option available)	Single 150W (AC only)	Single 750W*4	Dual 600W RPS
	100 - 240 VAC, 50-60Hz	80 Plus Platinum efficiency, 100 - 240 VAC, 50 – 60 Hz	
Power Consumption (Typical/Max)*3	57W / 75W	80W / 110W	180W / 240W
Heat in BTU/hour (Typical/Max)*3	195 / 256	273 / 376	615 / 819
Cooling Fan	Single Fixed Fan	Removable Fans	Hot Swap Smart Fans
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%		
Regulatory Certifications	FCC Class A, UL, CE, TUV, CB, VCCI, CCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI^, RCM^ | RoHS	FCC Class A, UL, CE, GS, CB, VCCI, CCC, KCC, BSMI, RCM | RoHS
Standard Warranty	90-Day Hardware and Software		

The specifications, performance numbers are subject to change without notice, and may vary depending on configuration and environmental conditions.

As for network interface, it's highly recommended to use A10 Networks qualified optics/transceivers to ensure network reliability and stability.

*1 Tested in single appliance SSLi deployment with maximum SSL option. Cipher "TLS_RSA_WITH_AES_256_CBC_SHA" with RSA 2K keys are used for RSA cases, "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256" with EC P-256 and RSA 2K keys are used for PFS case. | *2 With maximum SSL | *3 With base model. Number varies by SSL model | *4 Optional RPS available | *5 10Gbps speed only

^ Certification in process

SUMMARY

Traditional enterprise networks are not designed to cope with the rising demands of SaaS traffic. As organizations expand, with multiple branch office across the globe, user experience is severely deteriorated due to unoptimized traffic flow. Additionally, such deployments, coupled with a lack of visibility, can create major security problems like data theft.

A10 Networks' Cloud Access Proxy ensures that traffic flow at the branch offices, as well as the headquarters is optimized, improving network performance and enhancing the user experience. It provides tenant access control to stop data theft, as well as additional security features to ensure users and their data are protected. Maintaining full, centralized visibility across sanctioned and unsanctioned applications, at the branches, at the headquarters as well as the cloud further strengthens the security posture of organizations. The term-based subscription model provides greater flexibility and improves TCO.

NEXT STEPS

For more information, please contact your A10 Networks representative and visit: www.a10networks.com/cloud-access-proxy/.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19201-EN-03 DEC 2019