



SCALING AND SECURING OFFICE 365 APPLICATIONS WITH A10

AUGMENTING EXISTING PROXY SERVERS TO SCALE AND SECURE OFFICE 365 APPLICATIONS

A typical proxy server is neither designed nor optimized for highly demanding cloud applications such as Office 365. A10 Networks Thunder® devices can augment an existing proxy infrastructure and help it scale to keep up with the demands of Office 365 and other SaaS solutions.

Security and access control are some of the major concerns with Office 365 and other SaaS deployments. On-premise hardware solutions, such as A10 Thunder appliances, provide unparalleled performance, efficiency and security controls, along with traffic steering; features that are impossible to match with cloud-based solutions.

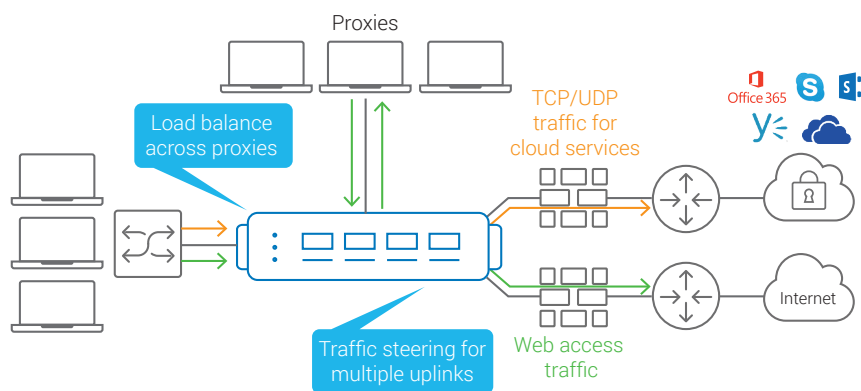


Figure 1: A10 Thunder devices augmenting existing proxy for Office 365

CHALLENGE

Office 365 poses tremendous scalability challenges when users open many dozens of long-lived, active connections and resulting increase in traffic can easily overwhelm an existing proxy. Security is equally important for compliance, as well as in preventing against unauthorized data access and exfiltration.

SOLUTION

A10 Thunder devices perfectly augment existing infrastructure to overcome the challenges introduced by a typical proxy. They can steer and intelligently route both TCP and UDP traffic to optimally utilize multiple uplinks while providing enhanced security features such as tenant access control and bidirectional SSL visibility.

BENEFITS

- Advanced traffic steering for multiple uplinks for optimal user experience
- Advanced NAT capabilities
- Tenant access control and SSL visibility
- Efficient load balancing across multiple proxies and uplinks
- Optional threat intelligence and URL classification services



CHALLENGE

A typical proxy server is neither designed nor optimized for highly demanding cloud applications such as Office 365. Office 365 creates a unique challenge in that each individual user creates dozens of long-lived connections to an Office 365 hosted environment. Additionally, large documents are now being transferred frequently to the cloud instead of being moved locally. These changes put significant strain on the local proxy server, which was not designed or sized for an Office 365 environment. Additionally, Microsoft recommends 2,000 clients use Network Address Translation (NAT) behind each public IP to ensure port limits are not reached.

Microsoft also recommends direct connectivity to Office 365 to provide faster and low latency performance.

Security is also a paramount concern for organizations utilizing SaaS technologies. Security measures such as access control are recommended to prevent against unauthorized data access and exfiltration, as well as for compliance reasons. For example, restricting access to personal Office 365 accounts and to known phishing and malware sites. In addition to access control mechanisms, more enterprises are investing in third-party monitoring tools such as firewalls, IDS, IPS and DLP systems to gain insight into their enterprise's encrypted traffic for inspection and policy enforcement. However, decryption is a resource-intensive task and can significantly degrade security appliances' performance, creating a chokepoint.

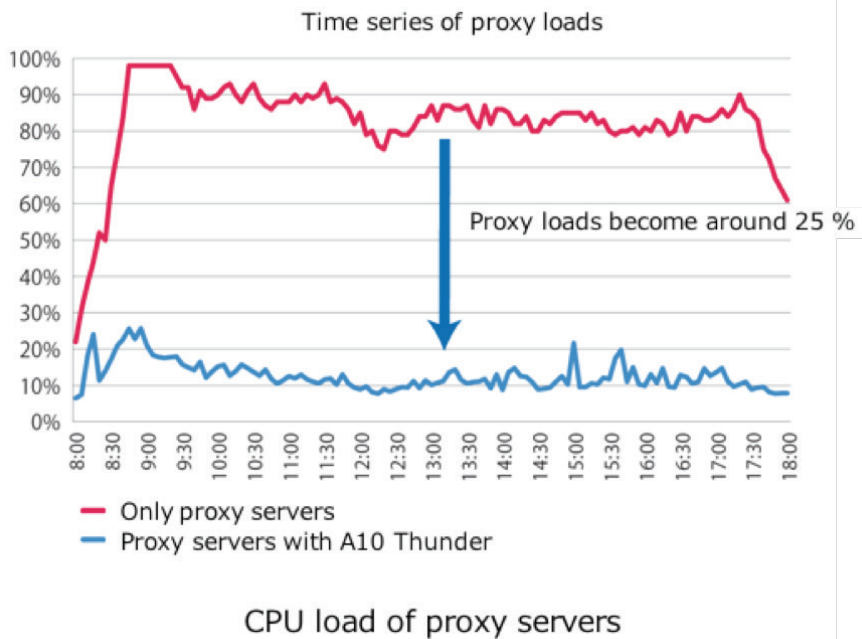


Figure 2: A10 Thunder device dramatically reduces proxy load induced by Office applications

A10 SOLUTIONS FOR OFFICE 365

A10 Thunder solutions are designed from the ground up for unmatched scalability and performance, and can meet any enterprise's requirements. A10 Thunder solutions simplify Office 365 deployments and can help save CAPEX and OPEX by consolidating functions such as load balancing, NAT and security capabilities.

As traffic and the number of devices grow, typical proxy infrastructure and NAT implementations can become bottlenecks. Security devices may suffer a similar fate due to significant performance degradation (up to 80 percent) while inspecting encrypted traffic, which has seen a sharp 75 percent increase.

A10 Thunder devices unleash the true potential of Office 365 by dramatically improving the user experience. A10 efficiently manages sessions and bandwidth while providing comprehensive security coverage for enterprise needs.

A10 Thunder solutions can reduce up to 75 percent of the load on your existing proxy infrastructure.

THE BENEFITS OFFERED BY A10 THUNDER SOLUTIONS INCLUDE:

- **Intelligent traffic steering** for bypassing existing proxies and to leverage the full potential of additional uplinks.
- **Load balancing** across multiple proxy servers and uplinks including for UDP traffic to efficiently utilize available resources.
- **Advance NAT capabilities** that allow oversubscription to exceed Microsoft's recommended 2,000 clients behind each public IP. Oversubscription is achieved by tearing down idle connections and by enforcing port quotas for clients. Other advance features allow public IP address stickiness by using the same IP address for all connections coming from the same client.
- **Bidirectional visibility with A10 Networks SSL insight® (SSLi®)** to scale your security infrastructure and utilize decrypt zones to decrypt once inspect multiple times.
- **Comprehensive tenant access control** for Office 365 and other SaaS solutions using A10 SSLi, which can perform real-time header insertion to prevent access to personal Office 365 accounts and only allow access to the corporate Office 365 tenant.

- **Optional threat intelligence and URL classification services** to further strengthen enterprise security and access control needs. URL filtering with URL classification services can block access to known botnets and malware sites while allowing access to other sites using URL categorization. Similarly, the threat intelligence service can block or white list IP addresses based on IP reputation.

SUMMARY

Office 365 introduces many new performance, scalability and security challenges. Existing proxy solutions are neither designed nor sized to meet this new set of challenges. A10 Thunder solutions augment existing proxies and provide significant performance improvements by acting as a force multiplier at a fraction of the cost. And they do so while providing much needed, comprehensive security coverage.

NEXT STEPS

For more information, please contact your A10 representative and visit: a10networks.com/firewall

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](https://twitter.com/a10Networks)

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

©2018 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, A10 Lightning, A10 Harmony and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.

Part Number: A10-SB-19179-EN-03 MAY 2018