BLUE COAT

Network
+ Security
+ Cloud

Using Blue Coat ProxySG to Secure and Enhance Office 365

SOLUTION BRIEF

Organizations around the world are migrating from on-premise Microsoft Office to cloud-based Office 365 deployments. As part of the migration process, Microsoft may suggest that Office 365 traffic bypass web proxy infrastructure. However, it's important to consider the security and network performance advantages lost if Office 365 traffic bypasses the proxy. Security advantages include: policy compliance, certificate status verification, application controls, logging, malware scanning, data loss prevention, and reverse proxy security for hybrid deployments. Network performance advantages include: lower firewall management costs, lower service disruption risk, content caching, IP address management, and connection optimization. This solution brief outlines the advantages offered by ProxySG to safeguard Office 365 traffic so you can make an informed decision regarding proxy bypass. In addition, the Blue Coat Mail Threat Defense solution provides specific security for email traffic associated with Office 365.

Security Advantages

Security Policy Compliance

Security best practice and most enterprise security policies prohibit direct Internet access from internal network clients. In other words, all client traffic, including Office 365, must pass through a proxy. This guidance exists for a reason – proxies provide valuable security benefits and we'll detail those benefits in the following sections. However, consistent policy compliance alone is an important consideration. Bypassing the proxy violates corporate mandates, forcing organizations to document an exception, justify the exception, and accept a lower security posture for this segment of Internet traffic. According to Verizon's 2012 Data Breach Incident Report, 97% of data breaches could be avoided with consistent implementation of simple or intermediate controls. Proxy bypass is a perfect example of inconsistent control implementation. Over time, accumulated exceptions are lost, becoming a source of security holes that attackers eventually exploit.

Certificate Status Verification

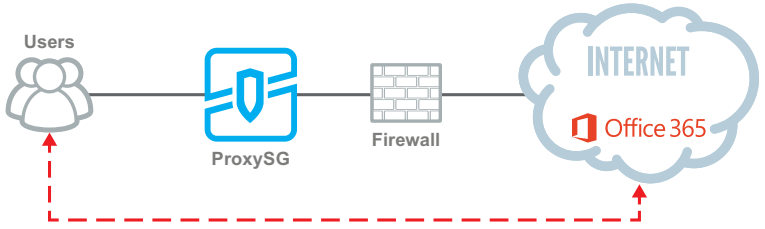
The reach of their software makes Microsoft a common target for certificate attacks. In fact, Microsoft certificate compromises known to the public have occurred in 2001, 2008, and 2012.[1] To protect your users against such attacks, Blue Coat ProxySG applies the Online Certificate Status Protocol (OCSP) to verify the status of Office 365 certificates in real-time. If a certificate has been compromised and revoked, the proxy blocks the request and alerts your users.

Full Incident Response and Compliance Logging

ProxySG also provides critical log data not available via Office 365 log records. For example, real client IP addresses are not recorded by Office 365. If an internal client uses Office 365, the source IP address will be NAT'd at the Internet Firewall. Therefore, if Office 365 traffic bypasses the proxy, it will not be logged, potentially resulting in compliance violations and limiting your ability to respond to attack incidents. To get true source addresses for users accessing Office 365 from behind any Network Translation entity, a proxy is required.

SSL Traffic

SSL visibility on the ProxySG provides complete visibility of encrypted Office 365 traffic. SSL blind spots are eliminated, so you gain visibility and control over SSL-encrypted traffic while giving you the ability to adhere to corporate and regulatory privacy policies.



Valuable security and network performance advantages are lost when Office 365 traffic bypasses the proxy.

[1] http://csrc.nist.gov/groups/SMA/forum/documents/october-2012_fcsm_pturner.pdf

BLUE COAT

Network
+ Security
+ Cloud

SOLUTION BRIEF

ADVANTAGES OF USING PROXYSG TO SECURE AND ENHANCE OFFICE 365	
SECURITY	NETWORK MANAGEMENT AND PERFORMANCE
Consistent policy compliance	Lower firewall operations cost
Certificate status verification	Lower service disruption risk
Web application controls	Content caching
Full breach response/audit logs	IP address management
Malware scanning	
Data Loss Prevention	
Reverse-proxy for hybrid deployments	
Web Application Control	

Reverse Proxy for Hybrid Deployments

Hybrid SharePoint deployments combine SharePoint Server resources with Office 365 SharePoint resources. In this case, search results from both sources can be combined to present users with a unified view of SharePoint resources in both locations. However, enabling this unified view requires inbound SSL connectivity from Office 365 to on-premise SharePoint servers. In this case, the reverse proxy capability of ProxySG can play an important role in securing these connections by providing an inbound SSL endpoint in the DMZ – authenticating, and decrypting traffic before passing it to SharePoint servers on the internal network. Direct (non-proxied) inbound connections from Internet resources should not be allowed to reach internal resources.

Network Performance and Management

Firewall Operations Costs and Service Availability

Firewall rule sets typically limit outbound Internet access to a single (or a few) static proxy IP addresses. Bypassing the proxy, however, requires that the firewall team open holes in the firewall from all client subnets to Office 365 IPs. To assist network managers in this task, Microsoft publishes the 175+ IP addresses necessary to support Office 365. However, these addresses constantly change. From January 2014 through August 2014, they changed 216 times. Therefore, bypassing the proxy commits your firewall team to manually synchronizing a firewall rule set covering 175+ constantly changing IP addresses – forever. This is a difficult task for any firewall team. Any time the rule set falls out of synch or simple misconfigurations occur, Office 365 services can be disrupted. Passing Office 365 traffic through the proxy completely avoids this firewall operations cost and availability risk.

Network Content Caching

Many organizations are concerned with increased bandwidth costs and latency associated with migrating from on-premise Office to Office 365 in the cloud. Because services in the cloud can have high latency, access to local content can make Office 365 applications much more responsive. The caching provided by the ProxySG will be particularly effective in Office 365 SharePoint and other environments in which the same objects (e.g. video, pictures, presentations, etc.) are downloaded by many users. In these environments, performance can be improved by up to 25%. If Office 365 traffic bypasses the proxy, these gains are lost.

IP Address Management

Microsoft recommends limiting the number of users behind each public IP address to less than 2000 users. Aggregating too many users behind a single IP creates port exhaustion problems that degrade performance. Depending upon your network design, compliance with this recommendation can be a challenge. While this requirement could be met with network restructuring, this process can be very disruptive and expensive. ProxySG can help you easily meet this requirement by load balancing users across a series of public IP addresses based upon various source selectors (e.g. client IP subnet).

More Information

Contact your Blue Coat representative for additional information on how ProxySG can help secure and enhance your Office 365 deployment.

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000