SOLUTION BRIEF

Using Symantec ProxySG to Secure and Enhance Microsoft Office 365

Symantec™

Introduction

Organizations around the world are migrating from on-premises Microsoft Office to cloud-based Office 365. As part of the migration process, Microsoft may suggest that Office 365 traffic bypass the web proxy infrastructure. However, it's important you consider the security and network performance advantages you will lose if Office 365 traffic bypasses the proxy.

Security advantages include:

- Policy compliance
- Certificate status verification
- Application controls
- Logging
- Malware scanning
- Data loss prevention
- Reverse proxy security for hybrid deployments
- SSL Visibility

Network performance advantages include:

- Lower costs of firewall management
- Lower risk of service disruption
- Content caching
- IP address management
- Connection optimization (see also Symantec MACH5)

So you can make an informed decision regarding proxy bypass, this solution brief outlines the ways the proxy-based Symantec secure web gateway solutions—including Symantec ProxySG and cloud-based Symantec Web Security Service—safeguard Office 365 traffic. In addition, Symantec email security solutions, including Symantec Messaging Gateway and Symantec Email Security.cloud, provide specific security for email traffic associated with Office 365.

Security advantages

Security policy compliance

Security best practices, 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, which we'll detail 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 it, and accept a lower security posture for this segment of internet traffic. According to Verizon's 2017 Data Breach Incident Report, 88 percent of data breaches follow patterns identified in 2014 by Verizon, and could be avoided if companies consistently implemented simple or intermediate controls. Proxy bypass is a perfect example of inconsistent control implementation: Over time, accumulated exceptions are lost, creating security holes that attackers can exploit.

Certificate status verification

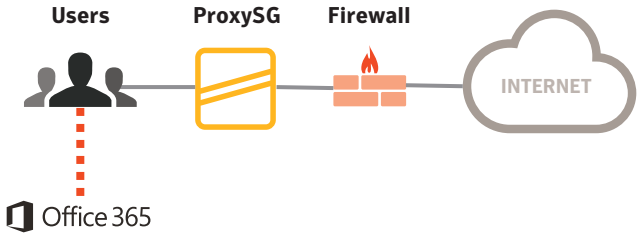
The reach of Microsoft software makes it a common target for certificate attacks. In fact, there were known compromises to Microsoft certificates in 2001, 2008, and 2012.[1] To protect your users from such attacks, Symantec Secure Web Gateway applies the Online Certificate Status Protocol (OCSP) to verify 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

Symantec ProxySG and Web Security Service also provide 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 attacks. To get true source addresses for users accessing Office 365 from behind any network address translation (NAT) entity, a proxy is required.

SSL traffic

The SSL visibility in ProxySG, Web Security Service, and the optional SSL Visibility Appliance give you complete visibility into encrypted Office 365 traffic. With SSL blind spots eliminated, you gain visibility into, and control over, SSL-encrypted traffic while also gaining the ability to adhere to corporate and regulatory privacy policies.



You lose valuable security and network performance advantages when Office 365 traffic bypasses the proxy.

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 and Office 365 SharePoint resources. Combining search results from both sources presents 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-premises SharePoint servers. 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 (nonproxied) 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 network operations team open holes in the firewall from all client subnets to Office 365 IPs. To assist network managers in this task, in 2014 Microsoft published 175+ IP address ranges necessary to identify Office 365 traffic. It was immediately apparent that these addresses would constantly change. In fact, from January through August 2014, they changed 216 times. As of November 2017, that number had jumped to 793 IPv4 ranges, representing approximately 2.7 million individual IPv4 addresses, plus 375 IPv6 ranges and 645 domain names.

Any time the rule set falls out of synch or simple misconfigurations occur, Office 365 services can be disrupted. Therefore, bypassing the proxy commits your firewall team to manually synchronizing a firewall rule set covering over 1,800 constantly changing IP ranges and domain names—forever. This places an enormous change control burden on the network operations team and introduces a large amount of preventable risk.

Passing Office 365 traffic through the proxy completely avoids this firewall operations cost and availability risk. ProxySG, through an Intelligence Services subscription, gets a direct updated feed of all the necessary IP addresses, domains, and app definitions directly from the Symantec Global Intelligence Network (GIN), keeping your organization's proxies up to date without manual changes to critical infrastructure. In addition, Microsoft has occasionally broken its own feed by accidentally excluding IP ranges for days at a time. When this happens, the Symantec GIN feed prevents these errors from impacting customers by serving the last known good data until Microsoft fixes the problem. Having the most up-to-date Office 365 information allows administrators to effectively implement policies on any Office 365 application—including the ability to whitelist, blacklist, bypass, or filter Office 365 applications—without concern for constant changes in Office 365 identifying traits.

Network content caching

Many organizations are concerned about increased bandwidth costs and latency associated with migrating traffic from on-premises Office applications to cloud-based Office 365. Make Office 365 applications much more responsive by providing access to local content (because services in the cloud can have high latency). ProxySG caching is particularly effective in Office 365 SharePoint and other environments in which many users download the same objects such as video, pictures, and presentations. In these environments, performance can be improved by up to 25 percent. 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 fewer than 2,000 users. Aggregating too many users behind a single IP creates port exhaustion problems, which degrade performance. Complying with this recommendation can be a challenge, depending on your network design. While you could meet this requirement with network restructuring, such a 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 on various source selectors, such as client IP subnet.

More information

Contact your Symantec representative for additional information on how ProxySG and Web Security Service can help secure and enhance your Office 365 deployment.

[1]NIST ITL July 2012 CA Compromise, Venafi
(http://csrc.nist.gov/groups/SMA/forum/documents/october-2012_fcsm_pturner.pdf)

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

SYMC_SB_ProxySG_Office365_v1.indd