BLUE COAT

Network
+ Security
+ Cloud

RESUMO DA SOLUÇÃO

Uso do Blue Coat ProxySG para proteger e melhorar o Office 365

Empresas do mundo todo estão migrando do Microsoft Office local para implementações do Office 365 na nuvem. Como parte do processo de migração, a Microsoft pode sugerir que o tráfego do Office 365 burle a infraestrutura de proxy da web. No entanto, é importante considerar as vantagens de segurança e desempenho da rede que serão perdidas se o tráfego do Office 365 burlar o proxy. Algumas das vantagens de segurança são: conformidade com políticas, verificação do status de certificados, controle de aplicações, registros, verificação de malware, prevenção contra a perda de dados e segurança de proxy reverso para implementações híbridas. Dentre as vantagens do desempenho de rede, podemos destacar: menores custos com gerenciamento de firewall, menor risco de interrupção do serviço, cache de conteúdo, gerenciamento de endereços de IP e otimização da conexão. Este resumo da solução descreve as vantagens oferecidas pelo ProxySG para proteger o tráfego do Office 365, para que você possa tomar uma decisão consciente quanto ao não uso do proxy. Além disso, a solução de defesa contra ameaças por e-mail da Blue Coat oferece uma segurança específica para o tráfego de e-mail relacionado ao Office 365.

Vantagens quanto à segurança

Conformidade com políticas de segurança

As práticas recomendadas e a maioria das políticas de segurança proíbem o acesso direto à Internet a partir de clientes de rede internos. Em outras palavras, todo o tráfego de clientes, inclusive do Office 365, deve passar por um proxy. Há um motivo para essa orientação: os proxies proporcionam benefícios importantes à segurança, e analisaremos esses benefícios mais detalhadamente nas seções as seguir. No entanto, a conformidade com as políticas é um fator importante a ser considerado. Burlar o proxy é uma violação às exigências corporativas, o que força as empresas a documentar uma exceção, justificá-la e aceitar uma postura de segurança menos rigorosa para esse segmento do tráfego da Internet. Segundo o relatório sobre incidentes de violação de dados (Data Breach Incident Report) de 2012 da Verizon, 97% das violações de dados poderiam ter sido evitadas com uma implementação consistente de controles simples ou intermediários. Burlar o proxy é um exemplo perfeito de uma implementação inconsistente de controles. Com o passar do tempo, perde-se o controle sobre as exceções acumuladas, que dão origem a brechas de segurança exploradas por invasores.

Verificação do status de certificados

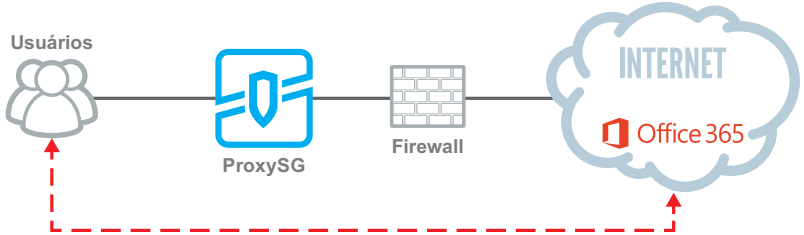
A popularidade do software da Microsoft faz dela um alvo comum de ataques de certificados. Inclusive, ocorreram comprometimentos de certificados da Microsoft divulgados ao público em 2001, 2008 e 2012.[1] Para proteger seus usuários desse tipo de ataque, o Blue Coat ProxySG aplica o Protocolo de status de certificados on-line (OCSP, Online Certificate Status Protocol) para verificar o status dos certificados do Office 365 em tempo real. Se um certificado for comprometido ou revogado, o proxy bloqueia a solicitação e alerta seus usuários.

Registros completos sobre resposta a incidentes e conformidade

O ProxySG também traz dados importantes de relatórios que não estão disponíveis nos registros do Office 365. Por exemplo, os endereços IP reais do cliente não são registrados pelo Office 365. Se um cliente interno utilizar o Office 365, o endereço IP de origem terá o endereço de rede convertido no firewall da Internet. Portanto, se o tráfego do Office 365 burlar o proxy, ele não será registrado, o que pode resultar em violações à conformidade, limitando sua capacidade de resposta a ataques. Para obter os verdadeiros endereços de origem dos usuários que acessam o Office 365 por trás da entidade de conversão de rede, é preciso ter um proxy.

Tráfego SSL

A visibilidade SSL do ProxySG proporciona uma visibilidade completa do tráfego criptografado do Office 365. Os pontos cegos de SSL são eliminados, para que você obtenha visibilidade e controle sobre o tráfego SSL criptografado e tenha a capacidade de cumprir as políticas corporativas e de privacidade regulamentares.



As importantes vantagens de segurança e desempenho de rede são perdidas quando o tráfego do Office 365 burla o proxy.

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

BLUE COAT®

Network
+ Security
+ Cloud

VANTAGENS COM O USO DO BLUE COAT PROXYSG PARA PROTEGER E MELHORAR O OFFICE 365	
SEGURANÇA	GERENCIAMENTO E DESEMPENHO DE REDE
Conformidade consistente com políticas	Menores custos operacionais com firewall
Verificação do status de certificados	Menor risco de interrupção dos serviços
Controles de aplicações da Web	Armazenamento em cache de conteúdo
Resposta a violações/registros de auditoria completos	Gerenciamento de endereços IP
Verificação de malware	
Prevenção contra a perda de dados	
Proxy reverso para implementações híbridas	
Controle de aplicações da Web	

Proxy reverso para implementações híbridas

As implementações híbridas do SharePoint combinam recursos do SharePoint Server com recursos do SharePoint do Office 365. Nesse caso, os resultados da busca das duas origens podem ser combinados para apresentar aos usuários uma visualização unificada dos recursos do SharePoint em ambos os locais. Porém, para possibilitar essa visualização unificada, é preciso ter conectividade SSL de entrada a partir do Office 365 para servidores do SharePoint no local. Nesse caso, a funcionalidade de proxy reverso do ProxySG pode ter um papel importante para a proteção dessas conexões, fornecendo um terminal SSL de entrada no DMZ, autenticando e descriptografando o tráfego antes de transmiti-lo aos servidores do SharePoint na rede interna. Não se deve permitir que as conexões de entrada diretas (sem proxy) de recursos da Internet tenham acesso aos recursos internos.

Desempenho e gerenciamento de rede

Custos operacionais de firewall e disponibilidade do serviço

Os conjuntos de regras de firewalls normalmente limitam o acesso de saída da Internet a apenas um ou a poucos endereços de IP de proxy estáticos. Porém, para burlar o proxy, a equipe de firewall terá de abrir brechas no firewall de todas as sub-redes clientes para os IPs do Office 365. Para ajudar administradores de redes nessa tarefa, a Microsoft publica mais de 175 endereços de IP necessários para compatibilidade com o Office 365 Contudo, esses endereços mudam o tempo todo. De janeiro a agosto de 2014, eles foram alterados 216 vezes. Portanto, burlar o proxy significa encarregar sua equipe de firewall de sincronizar manualmente um conjunto de regras de firewall que se aplica a mais de 175 endereços de IP em constante mudança, para sempre. Essa é uma tarefa difícil para qualquer equipe de firewall. A qualquer momento, se o conjunto de regras sair de sincronia ou houver um mero erro de configuração, os serviços do Office 365 podem ser interrompidos. Ao transmitir o tráfego do Office 365 pelo proxy, esse custo operacional com o firewall e o risco de indisponibilidade são evitados completamente.

Armazenamento em cache de conteúdo de rede

Diversas empresas têm preocupações com os maiores custos com largura de banda e latência relativos à migração do Office local para o Office 365 em nuvem. Como os serviços em nuvem podem apresentar alta latência, o acesso ao conteúdo local poderia fazer aplicações como o Office 365 serem muito mais responsivas. O armazenamento em cache oferecido pelo ProxySG será eficiente sobretudo para o SharePoint do Office 365 e outros ambientes em que o download dos mesmos objetos (por exemplo, vídeos, imagens, apresentações etc.) é feito por diversos usuários. Nesses ambientes, o desempenho pode melhorar em até 25%. Se o tráfego do Office 365 burlar o proxy, esses benefícios serão perdidos.

Gerenciamento de endereços IP

A Microsoft recomenda limitar, a menos de 2000, o número de usuários por trás de cada endereço IP público. Colocar usuários demais por trás de um único endereço IP traz problemas de esgotamento de porta que prejudicam o desempenho. Dependendo do design da sua rede, pode ser um desafio manter a conformidade com essa recomendação. É possível atender a essa exigência reestruturando a rede, mas esse processo pode causar muitas interrupções e gerar muitos custos. O ProxySG pode ajudá-lo a atender a essa exigência facilmente, realizando o balanceamento de carga dos usuários em uma série de endereços de IP públicos, de acordo com diversos seletores de origem (por exemplo, sub-rede de IP do cliente).

Mais informações

Entre em contato com seu representante da Blue Coat para obter mais informações sobre como o ProxySG pode ajudar a proteger e melhorar sua implementação do Office 365.

Sede Corporativa
Sunnyvale, CA USA
+1.408.220.2200

Blue Coat Brasil
São Paulo
+55 11 3443 6879

Blue Coat México
México D.F.
+52 55 3300 5825

Blue Coat Argentina
Buenos Aires
+54 (11) 4850 1215