Secure Internet Access via Zscaler in a Hybrid Network

Distributed Gateways: 9 design considerations for cloud-based Web Security

This whitepaper focuses on using Zscaler to secure your data while providing your users access to the high speed Internet they require, allowing IT to minimize risk while enhancing the user experience; bridging the gap between safety and freedom to roam.

orange™ Business Services

February 2016

Introduction

With the explosive growth of traffic to the Internet and the movement of mission critical applications to the cloud (such as Microsoft Office 365), IT organizations are struggling to provide a secure, responsive environment. At the same time, the security threats are also increasing exponentially with compromised client machines, trusting users (people-centric security[1]) and well-funded organizations (i.e., government or equivalent resources) launching more sophisticated attacks. While the traditional approaches for securing Internet access by using regional gateways and local breakouts have their merits, an approach where Internet traffic first goes through a cloud-based web security (SaaS) is becoming more attractive to global corporations.

SaaS based security companies such as Zscaler, Mobile Iron and others offer customizable and modifiable solutions that can be easily manipulated by a client side portal. The difficulty can lie in the implementation of the service as multiple components of the network architecture and the user profiles need to be considered prior to deployment. Key considerations include: security policies, firewall rules, authentication (SAML, ADFS, etc.), locations, browsers and groups to name a few. These and other points are reviewed in this paper.

Hybrid Networks: a disruptive force

Over the past year, our customers, which are primarily MNC's with sites around the world, tell us that their Internet traffic is growing at 50% per year and is now 40% to 80% of their total WAN traffic. Even those with very stringent security policies are considering modifications to the policy in light of the percentage of the traffic going to the Internet.

Cisco provides a more objective projection in their Cisco VNI Global IP Traffic Forecast, 2014–2019: "Business IP traffic will grow at a CAGR of 20 percent from 2014 to 2019. Increased adoption of advanced video communications in the enterprise segment will cause business IP traffic to grow by a factor of 2 between 2014 and 2019. Business Internet traffic will grow at a faster pace than IP WAN. IP WAN will grow at a CAGR of 9 percent, compared with a CAGR of 20 percent for fixed business Internet and 51 percent for mobile business Internet."

This is changing how we access the data and with that, shifting our traditional views on how we architect our infrastructure. The days of a single MPLS wide area network with a few Internet gateways are waning as we begin a transition to a hybrid solution that allows easier and cheaper access to the Internet. A hybrid network is a combination of different circuits (MPLS, Cable, Internet, 3G, 4G, etc.) that work collectively to provide the fastest route to our data. This leads to quicker delivery and better performance of our business-critical applications. By adding a layer of performance management tools, an optimized experience can be achieved and modified as needed to ensure consistency across all access technologies. This creates an efficient model for delivery but makes security difficult to implement and manage. However, the need for security is greater today than ever. How can an IT organization have both security and a more responsive WAN?

[1] http://www.gartner.com/smarterwithgartner/have-you-ever-considered-a-people-centric-security-strategy/

Securing your Internet: 3 types of solutions

Prior to the surge in Internet destined traffic, IT departments looked to consolidate Internet access to better control and secure Internet traffic. For global companies, this typically took the form of regional gateways that broke Internet traffic out from the VPN.

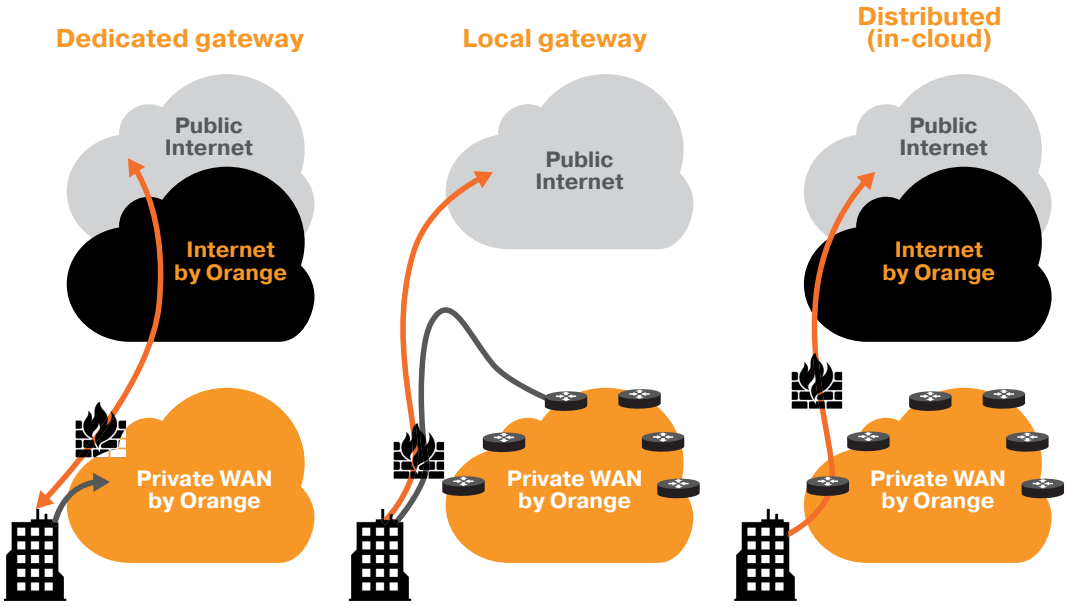
A limitation with the regional gateways is that as Internet use increases, it can cause congestion on the private network and potentially disrupt enterprise applications. In addition, because of the long physical distances between the user, the gateway and the destination site, the increased network latency can make some Internet applications virtually unusable.

In an attempt to solve these performance problems, many local IT departments reverted back to the approach of procuring Internet services from their local ISP. This eliminates central control of costs and a consistent global security policy. These traditional approaches to security introduced latency as each packet must be inspected in real-time. This causes throughput degradation in a multi-tenant environment for SaaS based applications. As a result, some vendors have lightened security measures to ensure speed of delivery, leaving access points open to attack.

With SaaS models changing the way we access our data, security platforms are adapting to accommodate the new delivery methods by adopting SaaS models themselves. These flexible solutions offer a critical advantage over traditional hardware or software based products as they are able to protect mobile devices in addition to PC's and servers with the same level of asset protection we have become accustomed to on the LAN side of the network. Safeguarding client side activity has become paramount to the security of our data.

Different models of Internet gateways can provide different levels of security, complexity and in some cases latency. Orange offers three different hybrid network configurations:

- Dedicated Gateways – hardware at your datacenter or our hosting center
- Local Gateways – cost effective and secure offloading of Internet traffic
- Distributed Gateways (in-cloud) – centralized, geo-located, secure and cost effective Internet access – using your security rules, all with no capex



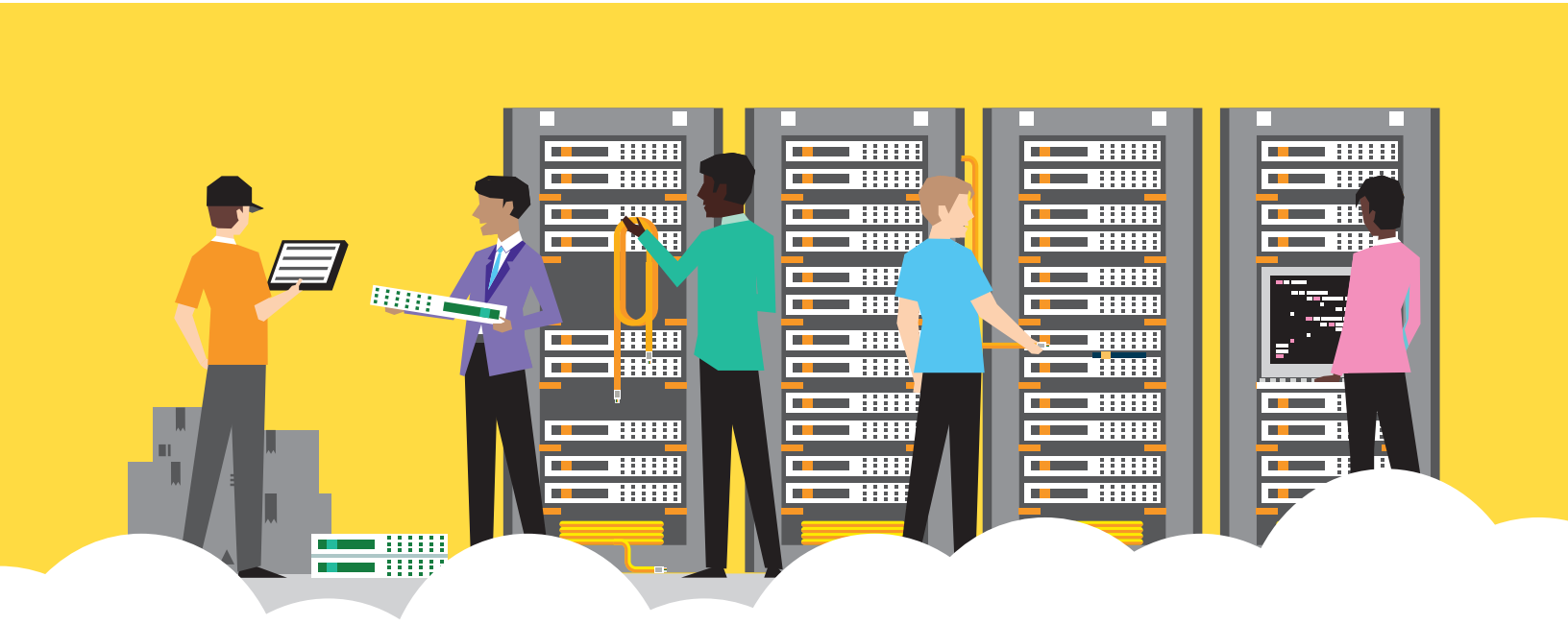
This whitepaper focuses on the distributed gateway model. Given that it is the most complex of the three, many of the principles can be applied to the other models.

Distributed Gateways: 9 design considerations for cloud-based Web Security

1. Traffic forwarding – during the planning phase, traffic forwarding patterns must be identified. They can be done explicitly (browser forwards traffic) or transparently (Internet gateway forwards traffic). This paper covers transparent forwarding as it is the more widely adopted mode of operation amongst Orange customers. In order to ensure proper configuration a few items must be addressed:

   - Routers must support Internet class-of-service – a major benefit of the hybrid network is the ability to pass Internet traffic through the MPLS network while realizing savings on the portion of MPLS traffic that is classified as Internet traffic. Routers must support Internet CoS in order to realize this benefit
   - Firewall rules must be written to allow Internet traffic to/from the Zscaler enforcement nodes, including authentication and reporting traffic where applicable
   - Primary and secondary Enforcement Nodes must be selected to ensure resiliency
   - It is imperative that IPSec tunnel parameters for transparent redirection of web traffic are determined and documented prior to roll-out. While some would use GRE tunnels, Orange strongly recommends the use of IPSec rather than GRE for a number of reasons
     - IPSec uses end-to-end authentication, making it very difficult for someone to masquerade as the Zscaler enforcement node for a man-in-the-middle attack
     - Cryptographic integrity control provides data protection
     - End-to-end encryption can be employed, should it be deemed necessary (though this is not often the case)
     - GRE is a stateless layer 3 protocol, making it possible to hijack a GRE session
2. Authentication – determine method (SAML, ADFS, etc.) and gather info needed prior to implementation
3. Zscaler parameters must be determined early in the planning stages

   - Locations – requirements and architecture are likely to vary with location. Traffic forwarding, authentication, bandwidth limits and other parameters may vary from site to site or even from subnet to subnet
   - Groups – differentiate groups that need Internet access from those who don't. Consolidation of groups is important, as managing many user groups is cumbersome and limitations can be reached. For example, a limited number of groups can be advertised to Zscaler



- Users – consider the type of users that will have Internet access: authenticated employees, unauthenticated consultants, mobile devices, etc. will likely have different security policies applied
- Devices – as with users, different devices may have different security policies applied. Reporting also needs to be taken into account with respect to what device-specific information is required
- Browser platforms and versions
- Features required to meet security policy
- Security policies
  - Web access
  - Anti-malware
  - File type control
  - Browser control
  - Advanced threat protection
  - SSL inspection
    - Some websites and services do not work well with SSL inspection. Test critical and commonly used sites
    - Certificate handling is complex and must be well understood for proper implementation
    - Cloud-based applications: instant messaging, streaming media, file sharing, social networking, blogging
  - Acceptance criteria

4. Internet firewall rules – it is likely that this implementation means moving off of existing firewalls to the firewalls at the Internet gateway. If so, it is easy to underestimate the effort of adapting the rule set to the new environment. The effort goes up considerably if the new firewalls are of a different brand than the ones in use. While there are translation tools, the output rule sets always require considerable human fine tuning, writing rules that did not convert and verification

5. Roles and responsibilities – this will reach across several groups within and outside your organization. A clear understanding of who is responsible for which activities is essential to success

6. Client side setup to review and anticipate:

   - Active Directory setup
   - Group Policy Objects
   - Browsers – there are differences between browsers that can impact how traffic is forwarded and how users are authenticated. The handling of SSL/TLS also varies from browser to browser. Close collaboration is required between desktop, Active Directory (or equivalent), security and teams to ensure all approved browsers are properly configured
     - Traffic forwarding: transparent forwarding, PAC files, manual proxy setting
     - Authentication
     - SSL certificates

7. Geo-location – when traffic gets redirected through distributed gateways, the source IP address may get translated. This can be misleading to the destination server or other services that rely on geo-location to determine the location of the original source of the request. Steps must be taken to preserve the origin IP address and ensure its geo-location lookup returns the proper source locale

8. MTU/MSS – as in any environment using encapsulation, setting the proper MTU and MSS size is essential to optimize performance

9. User experience (UX) – as this is a significant change, it is an easy target of blame for any hiccup on the network in the early stages of deployment. Take steps to minimize the UX impact. A stepped approach with minimal change at each step is best. A common (and tempting) mistake is to apply new security policies while you are configuring the new firewalls or implementing Zscaler. When users subsequently complain about failed access attempts, it will be difficult to determine if something is not properly configured or if it is a desired access restriction based on the new security policy. Make sure the newly implemented technology works properly before introducing changes that are not immediately required

Conclusion

Which security approach companies take to implementing hybrid network needs careful analysis. Planning is essential regardless of the Internet access architecture when implementing cloud-based web security such as Zscaler or a managed security service such as Orange Zscaler-based Web Protection Suite. In this whitepaper, Orange Business Services has shared some of the knowledge it gained in multiple hybrid network design and implementation projects. It is our hope that the lessons learned and discussed here will help our customers understand the thought processes and considerations that should go into a secure hybrid network plan.

About Orange Business Services

Orange Business Services, the Orange entity for business, is both a telecommunications operator and IT services company dedicated to businesses in France and around the world. Our 20,000 employees support companies, local government bodies and public sector organizations in every aspect of their digital transformation. This means we're at hand to orchestrate, operate and optimize: mobile and collaborative workspaces; IT and cloud infrastructures; connectivity (fixed and mobile networks, private and hybrid systems); applications for Internet of Things, 360° customer experience and big data analytics – as well as cybersecurity, thanks to our expertise in the protection of information systems and critical infrastructures. More than 2 million businesses in France and 3,000 multinationals place their trust in us. See why at: orange-business.com or follow us on Twitter @orangebusiness.

orange™ Business Services