Solution Brief

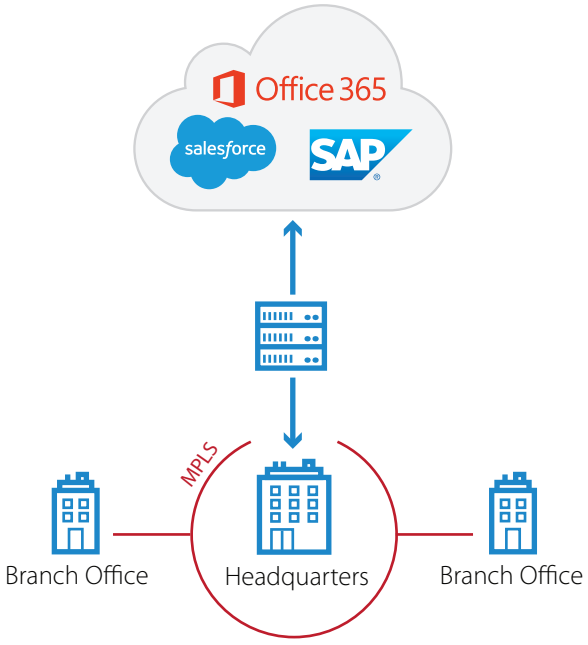
Barracuda Web Security Service

Barracuda Web Security Service is a cloud-based service that delivers complete Internet and web security. Unlike traditional centralized approaches, it allows organizations to connect directly to the cloud and minimize appliance and network infrastructure. Built for maximum performance and cloud intelligence, the Barracuda Web Security Service can cost-effectively scale security to all offices or users, regardless of location.

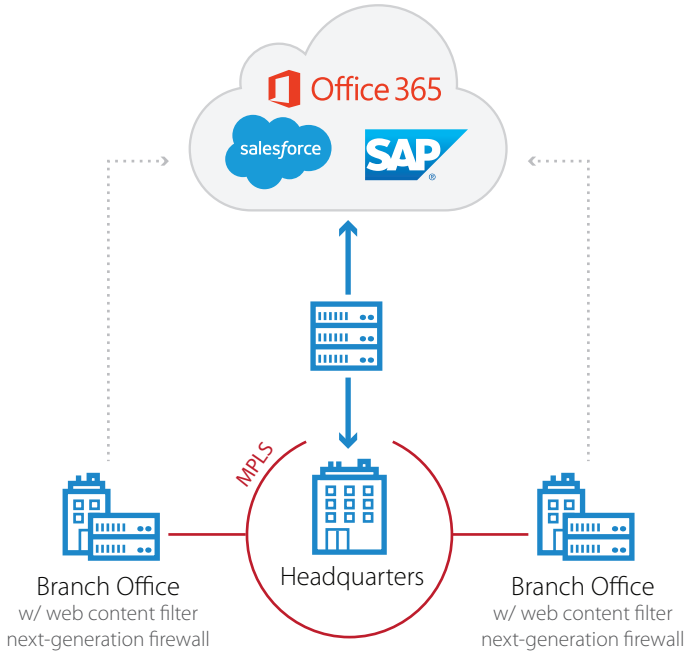
The Cloud-First World is Changing Perimeter Security

Corporate networks have been seeing significant changes in traffic flows. Applications are moving out of the data center and the Internet has become the primary destination. This change presents you with two challenging network choices for securing branch and mobile user traffic: backhauling traffic (known as "hub and spoke") or deploying appliances in each location.

Both of these traditional architectures have pros and cons in a cloud-first world. Taking dispersed remote office traffic and backhauling it to centralized security appliances is expensive and complicated. Alternatively, deploying appliances at every office location can be time-consuming and potentially more expensive to maintain. Furthermore, mobile users often bypass both these architectures by disabling their cumbersome VPNs and going straight to the cloud, which leaves much of your user traffic uninspected.



Classic Model Hub and Spoke
Expensive to backhaul and scale
poor user experience

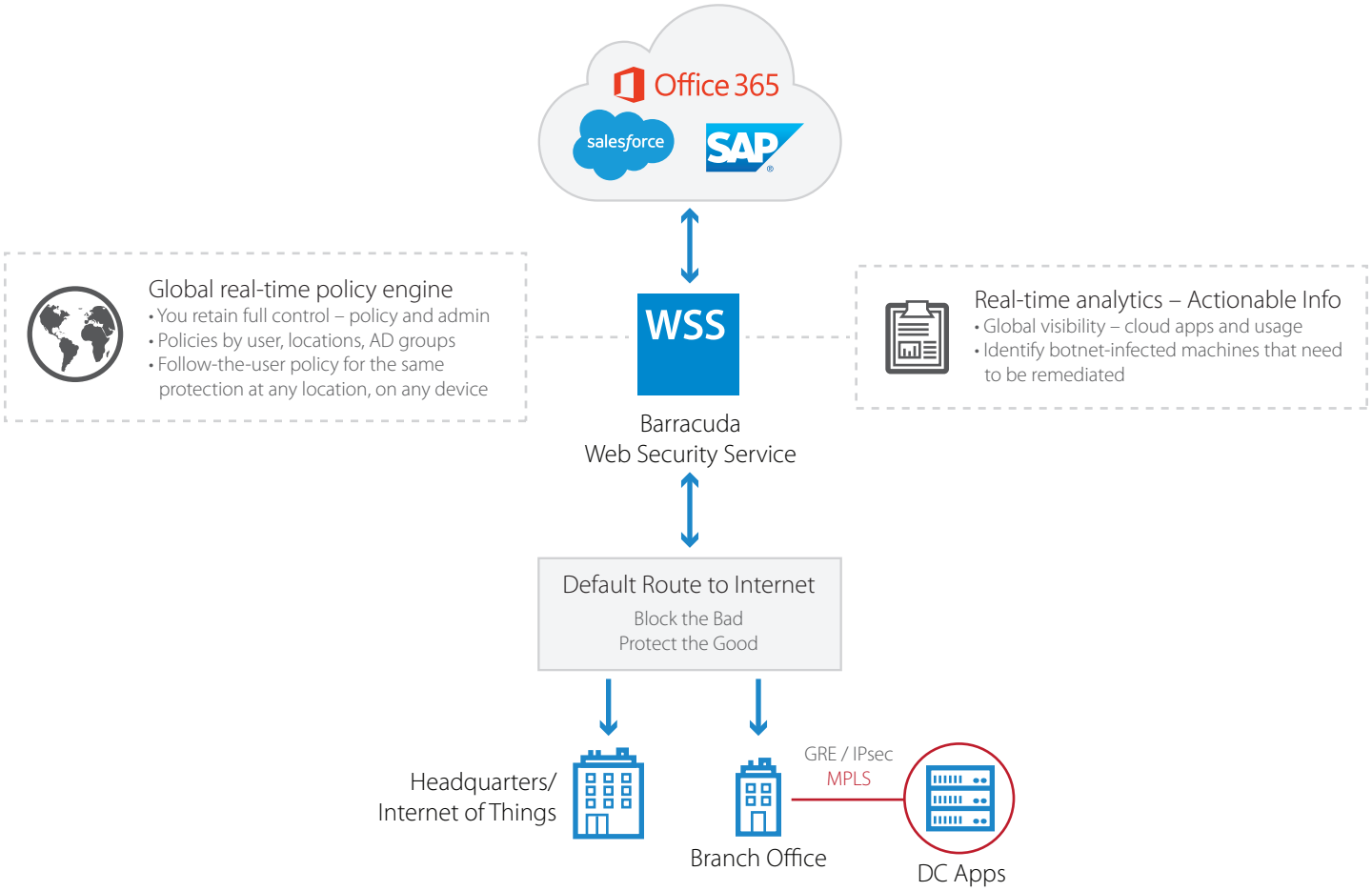


Appliances
Distributed model can be time consuming
and expensive to deploy and maintain.

Direct-to-Cloud™ Access

Barracuda Web Security Service enables you to connect your offices or users directly to provide better performance, minimize appliance infrastructure, and reduce costly MPLS backhauling. Through our partners, we use over 100 data centers worldwide—your first stop to the Internet begins by connecting to Barracuda Web Security Service. We do the rest and provide you with a cloud-based security stack that is completely integrated for maximum protection.

The solution sits inline and inspects every byte of traffic across 12 different security techniques, so you get full protection from web and Internet threats.



All these capabilities are delivered by the Barracuda Web Security Service, powered by the world's largest security cloud, which processes more than 30 billion requests a day. Any threat detected within the global platform is immediately blocked for all other customers across the entire cloud.

Customers can assign unified policies, and the policies will follow users regardless of location. When a policy change is implemented, it immediately cascades across the entire cloud upon the next security transaction. In addition, the patented NanoLog technology provides a 50:1 compression on security logs, delivering near real-time reporting across the cloud.

Access Control

Controlling what your users access, and how they access it is a key first step to strengthening security and restricting malicious traffic habits. Our Internet access provides an integrated suite of technologies that allow you to take action before threats take hold, allowing you to easily manage your network traffic.

URL Filtering

With just a few clicks, you can block or limit website access based on a user, group, or location for a single URL or across any of our 90 URL categories, 30 super categories, and six classes. For any URL that is not already classified, Barracuda uses a Dynamic Content Classification (DCC) engine to scan the page for any content that would place it in a predefined category.

Threat Prevention

Barracuda Web Security Service uses a ByteScan engine to scan every byte of traffic in parallel across multiple threat engines in real time. Parallel scanning provides great performance with near-zero latency, while accelerating the discovery of threats in your traffic. Because it's delivered from the cloud, any threat discovered across our millions of users is immediately blocked for everyone else in our cloud.

Advanced Protection

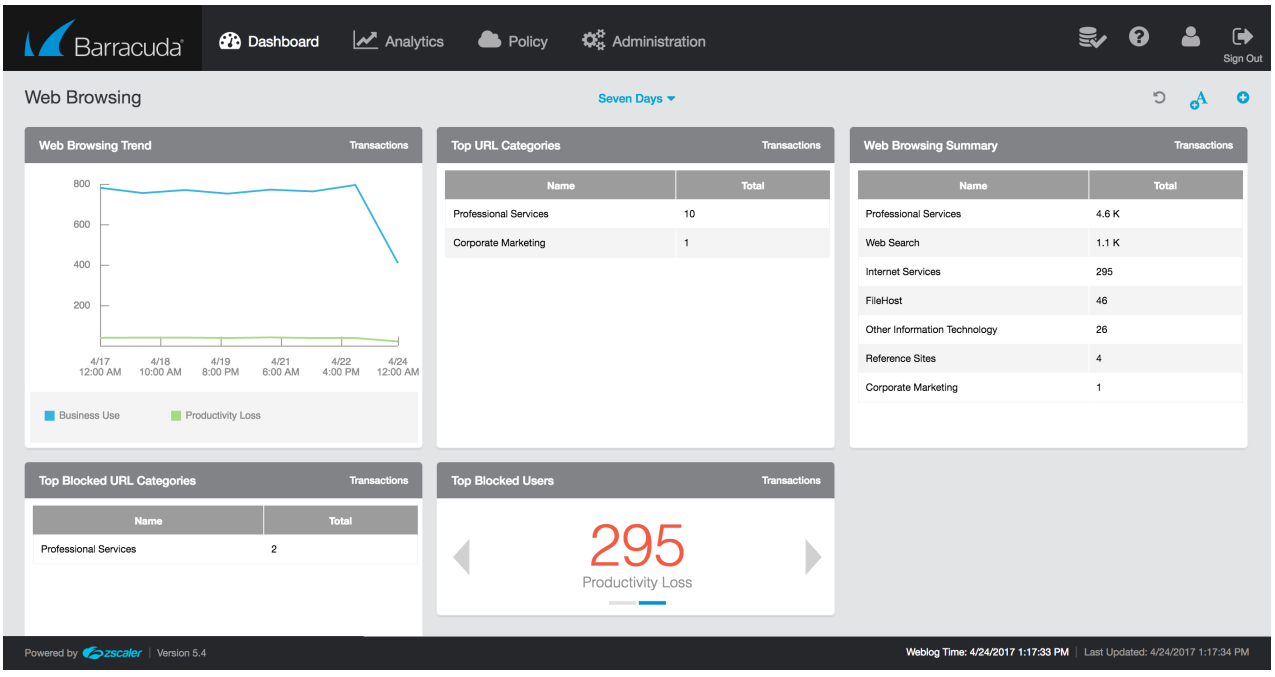
Barracuda Web Security Service delivers real-time protection against malicious web content by employing risk-based analysis of all content access by a user. You can block browser exploits, injected scripts, vulnerable ActiveX, zero-pixel iFrames, as well as identify botnets and malware callbacks that are operating in your network. Cross-site scripting, fraud protection, cookie stealing, and suspicious tunneling can also be identified and blocked.

Anti-Virus

The Barracuda Web Security Service provides anti-virus, anti-spyware, and anti-malware protection for all users, using signatures sourced from over 40 threat intelligence sources. As a member of the Microsoft Active Protections Program (MAPP), Barracuda Web Security Service regularly gets and updates signatures across our cloud before they are made public—you get all the security without any of the signature update headaches.

Complete Control, Visibility, and Reporting

The Barracuda Web Security Service uses a single, unified console to create Internet and web policies across access control, application prioritization, threat prevention, and data protection. Policy changes are instantly applied across the entire cloud. The policy console provides real-time insight to view and analyze all traffic across all devices and locations. It's easy to drill down to a per-user overview to locate a botnet-compromised device, or leverage the application visibility to validate if and where non-IT–compliant apps are used.



Barracuda Packages

Barracuda offers complete Internet and web security in convenient subscription suites or a-la-carte:

Edition Comparisons	Basic	Advanced
Inline Anti-Virus and Anti-Spyware		
Signature-based anti-malware protection for any file size	•	•
Full inbound/outbound file inspection with near-zero latency	•	•
True file type by users, groups, and destinations	•	•

Edition Comparisons Cont.	Basic	Advanced
Web Access Control		
Ensure outdated versions of browsers are forced to upgrade	•	•
Ensure known browser vulnerabilities are patched	•	•
Mobile Applications and Devices		
Granular reporting of mobile applications and device types	–	•
Security policy for mobile applications	–	•
Cloud Application Controls		
Granular application controls (i.e., allow viewing/block uploads)	•	•
Streaming media - YouTube, Hulu, Google video, etc.	•	•
Social networking and blogs - Facebook, Twitter, Orkut, etc.	•	•
Webmail and Web IM - Gmail, Yahoo mail, Hotmail, etc.	•	•
Collaboration, business applications	•	•
Advanced Threat Protection		
Block malicious code, spyware, and viruses from infected sites	–	•
Real-time feeds of phishing, botnets, and other malicious sites	–	•
PageRisk to stop botnets, XSS, and malicious active content	–	•
Block Anonymizer, ToR, P2P, Skype, Gtalk and Gizmo	–	•
Standard Behavioral Analysis	–	•
SSL Inspection		
SSL inspection of any content with 2048 bit certificate support	•	•
Granular policy for exclusion of content to be inspected	•	•

Note: There are limited advanced threat protection elements included in the Basic suite. Please see below chart for a full list:

*Advanced Threat Protection (ATP) Features	Basic	Advanced
Botnet protection (C2 servers)	•	•
Botnet protection (C2 traffic)	–	•
Cross-site scripting (XSS) protection (cookie stealing; potentially malicious requests)	–	•
Fraud protection - known phishing sites	•	•
Fraud protection - suspected phishing sites	–	•
Fraud protection - spyware callback	–	•
Fraud protection - web spam	–	•
Malicious active content protection - browser exploits	–	•
Malicious active content protection (malicious content and sites, vulnerable ActiveX controls, file format vulnerabilities, blocked malicious URLs)	–	•
P2P file sharing protection (BitTorrent)	•	•
P2P anonymizer protection (Tor)	•	•
P2P VoIP protection (Google Talk, Skype)	–	•
Suspicious content protection (PageRiskTM)	–	•
Suspicious destinations protection (blocked countries)	–	•
Unauthorized communication protection (IRC tunneling)	–	•
Unauthorized communication protection (SSH tunneling)	–	•
Unauthorized communication protection (Anonymizers)	•	•

Cloud-Based Security

The cloud-based platform has been purpose-built to provide comprehensive, multilevel security and access control that is 100 percent in the cloud.

Our Web Security Service enables an organization to up-level its security posture without the cost and complexity of stacks of appliances. By moving the security stack to the cloud, we protect users everywhere they go, with policy-based access and inline protection from malware and other threats. It also enables organizations to provide secure local breakouts and simplify the rollout of applications like Office 365 so they can embrace the benefits of the cloud and mobility.

The Barracuda Web Security Service also works perfectly in conjunction with the Barracuda NextGen Firewall, allowing your firewall to offload services like web content inspection and SSL scanning and reporting. Doing this ensures a unified, comprehensive web and network security, while maintaining firewall performance across any number of locations, without compromising security effectiveness.