Quick Start 5: Introducing and configuring Websense® Cloud Web Security solution

Websense Support Webinar April 2013

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

Presenter

Greg Didier

- Title:
  - Support Specialist
- Accomplishments:
  - 9 years supporting Websense products
- Qualifications:
  - Technical Support Mentor
  - Product Trainer

Goals And Objectives

websense

- Understanding the *in-the-cloud* concept
  - **S**oftware **a**s **a** **S**ervice (SaaS)
- Web Cloud Security requirements
- Deployment options
- Setup and configuration steps
- I will consider my job successful, if after watching this presentation, you feel confident knowing how to get our Cloud Web service up and running.

Websense Cloud Platforms

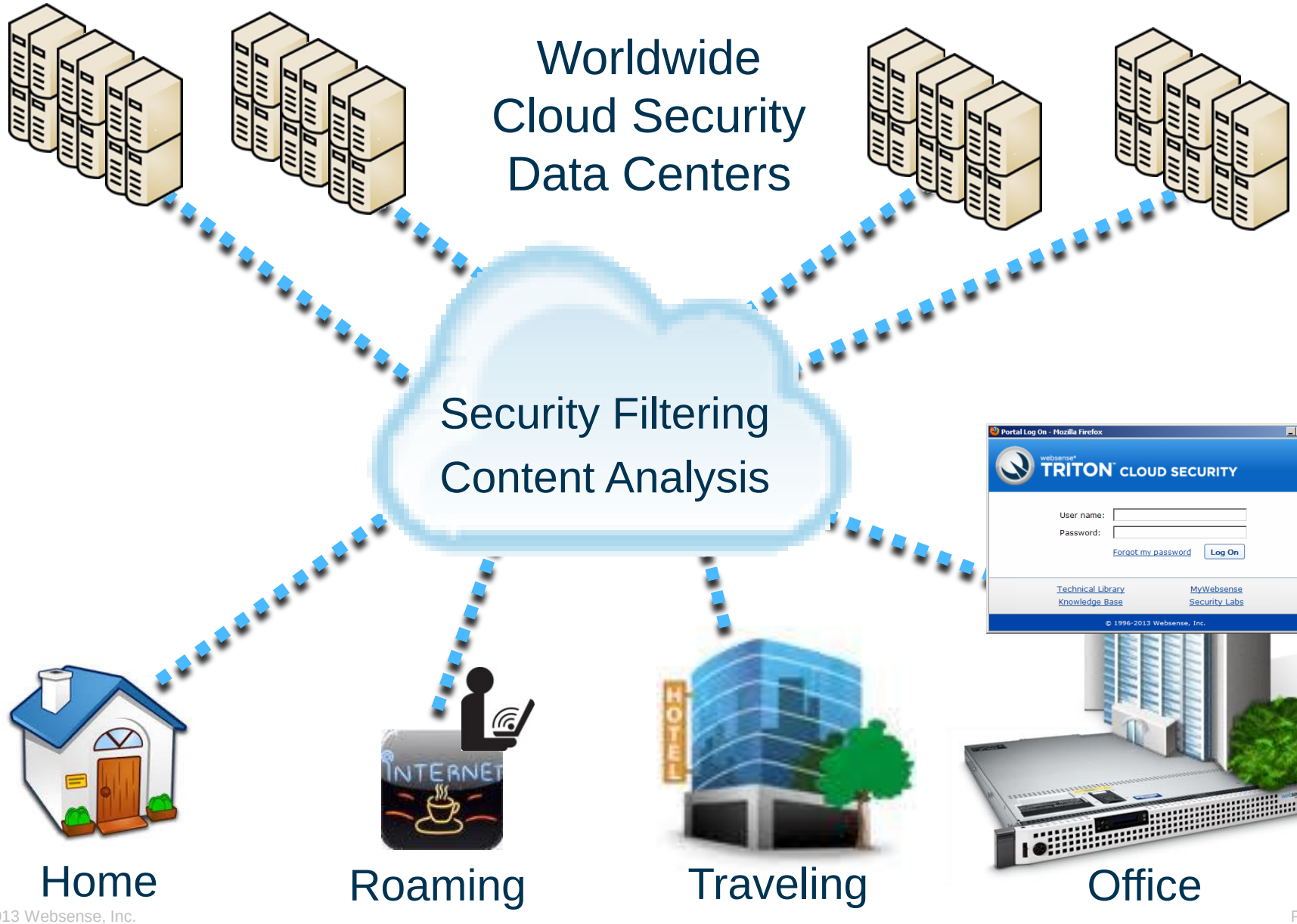
- Cloud Email Security
  - Email is cleansed before it reaches your network.
- TRITON™ Mobile Security
  - Unified security solution for content-aware data, web, malicious app protection, and mobile device management.
- Cloud Assist (new)
  - Provides on-premises URL analysis and application/protocol detection for Web traffic, along with centralized policy management and reporting capabilities in the cloud.
- ACE in the Cloud
  - Runs Websense analytics on your incoming Internet traffic.
- **Web Security Gateway Anywhere**
  - Combines on-site and in-the-cloud security.
- **Cloud Web Security Gateway**
- **Cloud Web Security**

Platform Names

- Websense® Cloud Web Security Gateway
  - Your SSL proxy, analytics, and Cloud security protection
  - Commonly known as ‘Cloud Web Security Gateway’
- Websense® TRITON™ Cloud Web Security
  - Your Cloud security protection
  - Commonly known as ‘Cloud Web Security’
  - Formally known as Websense Hosted Web Security
- Hybrid (in-the-cloud)
  - Combines cloud-based and on-premises filtering
    - Web Security Gateway Anywhere (V-Series appliance)
    - Cloud Web Security Gateway
  - Create policies for on-premises and hybrid filtering in a single console—TRITON - Web Security

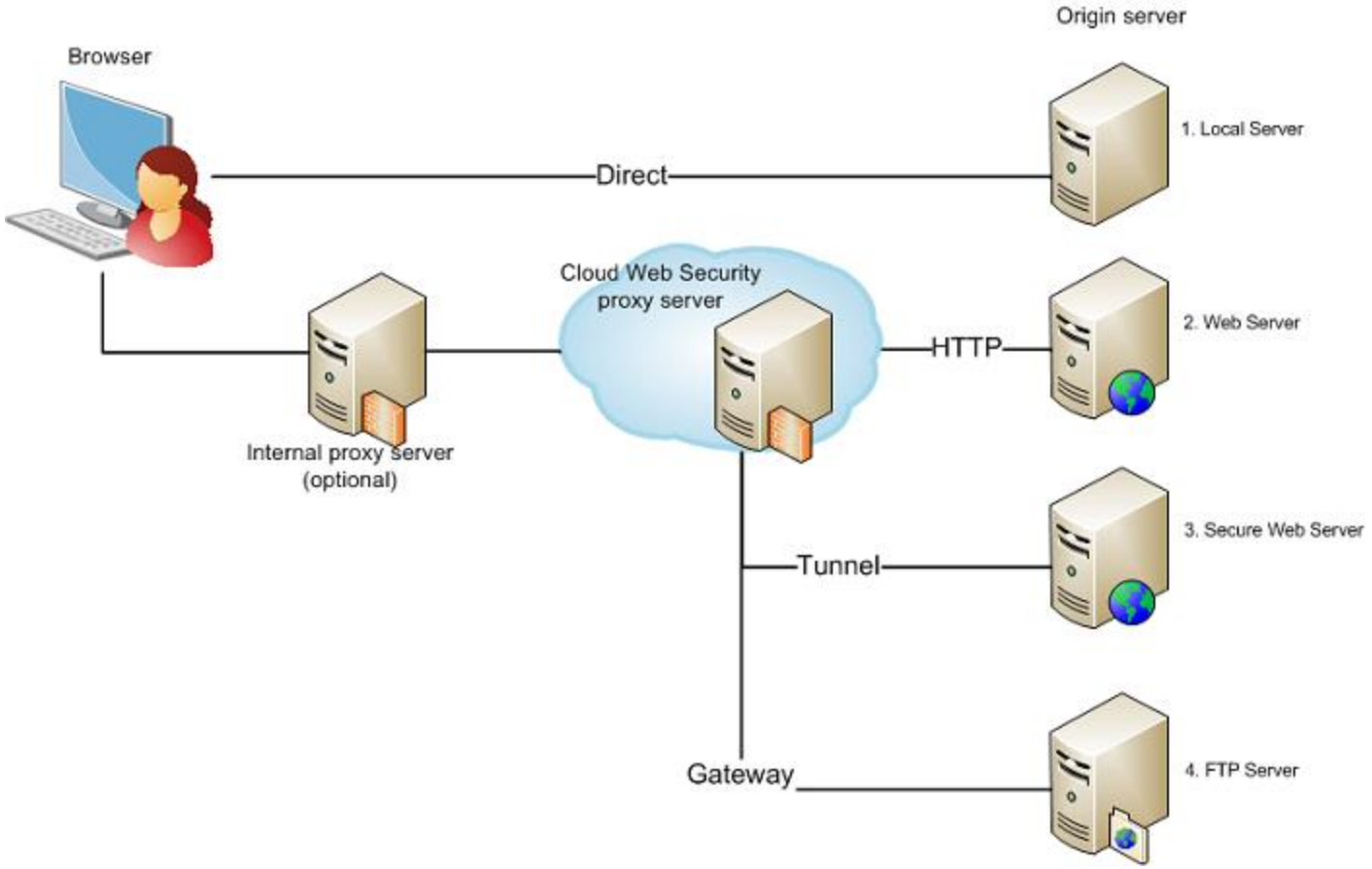
Software As A Service

websense



Websense Cloud Web Security

- Websense Cloud Web Security operates as a proxy service for HTTP, Secure HTTP (HTTPS), and FTP over HTTP.



Platforms Covered In This Webinar

- Websense Cloud Web Security
  - 15 worldwide data centers
  - Web Security and Filtering
  - ThreatSeeker® Network
  - Office, remote and mobile users
- Websense Cloud Web Security Gateway
  - 15 worldwide data centers
  - Web Security and Filtering
  - ThreatSeeker® Network
  - Office, remote and mobile users
  - Web Proxy + SSL inspection
  - Cloud Endpoint Agent
  - Social Web Controls
  - Executable file analysis
  - Advanced Classification Engine (ACE)
    - Real-Time Content Classification
    - Real-Time Security Classification
    - Antivirus File Analysis
    - Advanced Detection File Analysis
    - Rich Internet Application Analysis

Getting Started

- Five steps
  1. Request a Cloud Web Security account
  2. Select a deployment method
  3. Identify your gateway (external IP address)
  4. Configuring your Firewall for Cloud Web Security
  5. Set up authentication (optional)

Enabling Cloud Web Security

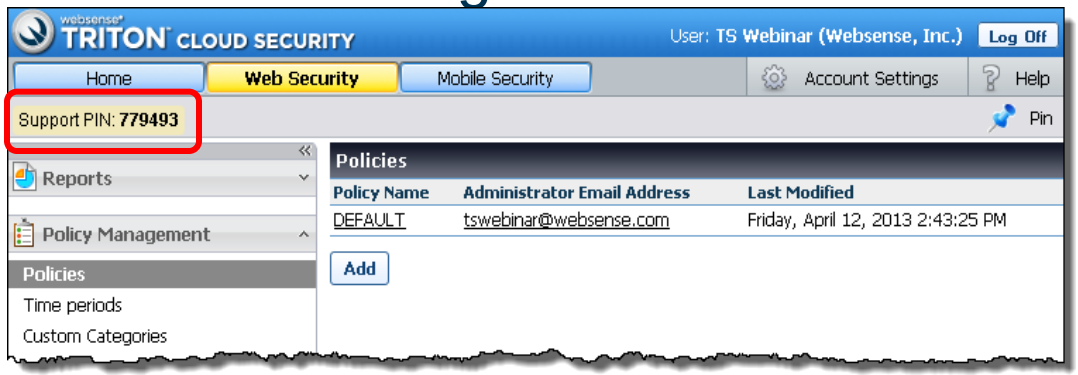
- Request an evaluation
  - Visit www.websense.com
  - Select Products > Web Security > Request A Trial
- Register for *Cloud Web Security Gateway*
  - Click the registration link in your confirmation email
  - A security check takes 24 business hours
- Log on to the Cloud Security portal
  - Visit www.mailcontrol.com/login/login_form.mhtml
  - Activate your trail license—accept the license agreement

Enabling Cloud Web Security

www.mailcontrol.com/login/login_form.mhtml

Recap: Enabling Cloud Web Security

- Request an evaluation
- Register for *Cloud Web Security Gateway*
  - Security check
- Log on to the Cloud Security portal
  - Configure Cloud Web Security via the Web portal
  - Default policy is active
    - Web Security > Policy Management > Policies
- Demonstration
  - Enable and test Cloud filtering



Recap: Demonstration

Cloud Security
Data Center

Web
Content

Known source
IP address:
204.15.64.97

Corporate Office

Unknown source
IP address

Off site

To determine if a user is roaming, Cloud Web Security uses the source IP address.

Deployment

- Decide how you will be sending Web content requests to Websense Cloud Security?

Home

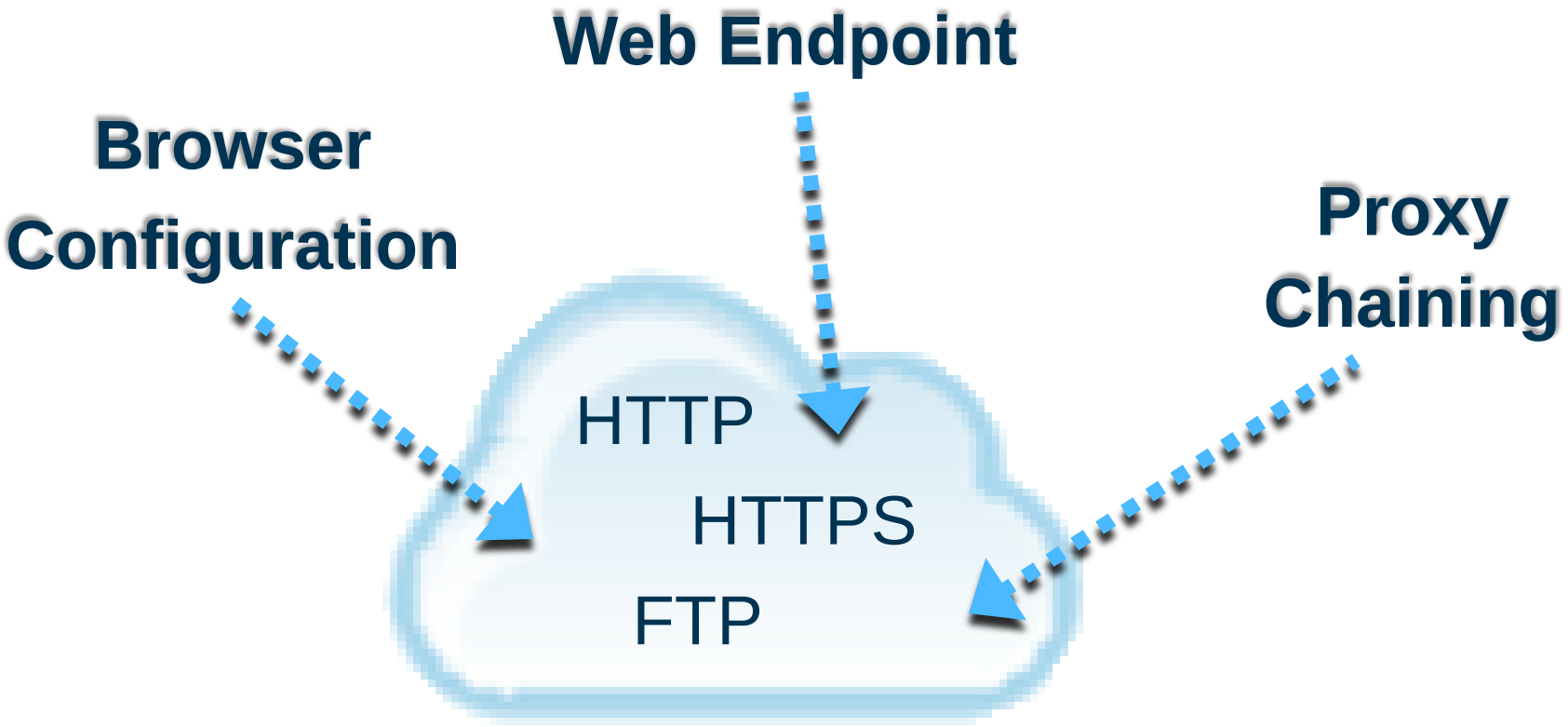
Roaming

Traveling

Office

Selecting A Deployment Method

- Websense Cloud Web Security operates as a proxy service



- HTTPS traffic tunnels unless decryption is enabled
  - Requires distributing a root certificate to client machines

Select Deployment Method

- You must direct Web requests to the Cloud service
- Proxy chaining
  - If you already have a internal proxy server
    - Direct it to use Cloud Web Security in a chained proxy configuration
- Configure browsers
  - Proxy automatic configuration (PAC) file
    - Defines an appropriate proxy for fetching a given URL
    - Easily deployed and configurable for entering exclusions
  - Group Policy Object (GPO)
- Websense Web Endpoint
  - Agent passes authentication information and requests a PAC file to force use of Cloud Web filtering

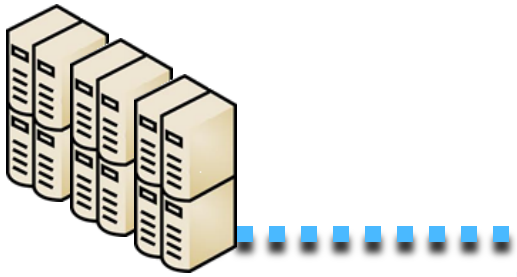
Proxy Chaining

- Configure your existing proxy
  - Forward http, https, and ftp requests
  - Basic chaining
  - NTLM pass-through
  - X-Authenticated-User
- If your proxy is capable of using a PAC file
  - Use the one provided by Cloud Web Security
- If your proxy is not capable of using a PAC file
  - Download a copy of the Cloud Web Security PAC file and duplicate its functionality
    - If you make policy changes and are not using the PAC file in your proxy, you must update your proxy configuration to match

Browser Configuration Via PAC file

- Browsers must get their PAC file from the Cloud Web Security service
  - Specify either a standard or a policy-specific PAC file
- Standard PAC file
  - Non-policy specific
    - http://webdefence.global.blackspider.com:8082/proxy.pac
  - Typically used for all users
- Policy-specific PAC file
  - Specified in the browser
    - Ensure user receives correct PAC file regardless of location
  - Listed in the General screen for each policy, for example:
    - http://webdefence.global.blackspider.com:8082/proxy.pac?p=xxxxx
  - Useful for roaming users

Recap: Policy-specific Or Standard PAC File



Security Filtering
Content Analysis

- Standard Pac file
  - All requests go to the Cloud Service
  - If user cannot log into the Cloud service, he cannot access the Internet
  - Problematic for lost passwords

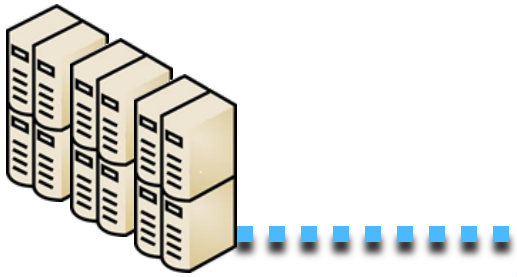
Standard PAC File:

No custom URL exceptions

Unknown source IP address

Roaming user

Recap: Policy-specific Or Standard PAC File



Security Filtering
Content Analysis

- Policy-specific Pac file
  - Allows entering exceptions for direct Web access
  - Allows accessing corporate email to retrieve forgotten passwords

Policy-Specific PAC File:

Contains your custom URL exceptions

Unknown source IP address

Roaming user

Endpoint Client

- For Hybrid and Cloud Web Security Gateway
  - Not available for Cloud Web Security
- Ensures users are both authenticated and always filtered by Cloud Web Security
- Supports 32-bit and 64-bit Mac or Windows operating systems
- Incorporates protections against tampering
- Optional auto-update feature

Endpoint Client Deployment

- Define an anti-tampering password
- Download endpoint installer
- Deploy endpoint client
  - Active Directory group policy object (GPO)
    - `msiexec /package "\\path\Websense Endpoint.msi" /quiet /norestart WSCONTEXT=xxxx`
    - **path** - is the path to the unzipped installer
    - **WSCONTEXT=xxxx** – from the Endpoint Download screen
      - Associates endpoint clients with your customer account
  - Manually via command line
    - `msiexec /package "Websense Endpoint.msi" /norestart WSCONTEXT=xxxx`
  - Deploy from cloud or hybrid service
- Demonstration

Firewall Ports

- Minimum open ports
  - 80
    - Unproxied home page and other direct Cloud support URLs
  - 80 or 8082
    - Browser or proxy requests for the PAC file
  - 80 or 8081
    - Provides the Cloud Web Security service
  - 80 and 443
    - Cloud Security administration Web portal
- Additional open ports
  - 8088 and 8089
    - Authentication service and secure form-bases authentication
- Cloud Cluster IP address
  - Cloud Service cluster IP addresses and port numbers

Applying Policies

- Identify the correct policy
  - Checks source IP address
    - Match Proxied Connections setting in a policy
  - Web Endpoint passes authentication details
  - Login with email address
    - Must be unique

Hybrid – Appliance Tips

- Hybrid
  - Unified on-premises software and off-site hybrid service
- Appliance sends policies to the hybrid service
- Cloud Web Security cannot apply polices based on source IP address
- Hybrid/Cloud can only authenticate synched users

Additional Tips

- Stop other applications from bypassing the service
- Non-Proxied Destinations (exceptions)
  - Can be a domain name, an IP address, or an IP subnet
  - Entries automatically appear in the PAC file
  - Add your corporate Web email address and known good external resource sites
- Visiting another company
  - Another company's policy may apply. Because you are not a user registered from the source IP address, you can neither log on nor register. Contact the company's Web policy administrator for access.

Additional Tips

- Roaming users
  - Set the home page of roaming users to
    - http://home.webdefence.global.blackspider.com
    - This URL is requested over port 80
    - Cause hotel firewall to respond with the payment page
  - Configure browsers with policy-specific PAC file
    - Your Non-Proxied Destinations are in the PAC file
  - Cloud Web Security works on the basis of source IP

Cloud Web Security Links

- Getting Started Guide
- TRITON™ Cloud Security Help
- Websense® Cloud Web Security datasheet
- Websense® Cloud Web Security Gateway datasheet
- Product Comparison Chart
- Working with Remote Users
- How do I probe or query the Cloud Web Security service?

Upcoming Webinar

websense

Webinar Update

Title: Quick start 6: Administering the Websense® Cloud Web Security solution

Date:

May 22, 2013

Time:

8:30 A.M. PST (GMT -8)

How to register:

www.websense.com/content/SupportWebinars.aspx

Training

- Websense Training Partners offer classes online and onsite at your location.
- For more information, please send email to: readiness@websense.com
- To find Websense classes offered by Authorized Training Partners in your area, visit: www.websense.com/findaclass