websense®

Greg Didier

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

Goals And Objectives

- Examine the new features in version 7.7
  - TRITON Management Server
  - New in Websense Web Security
  - New in V-Series Appliance
  - New in Websense Content Gateway
  - Introducing Mobile Security
- Make you aware so that you can take advantage
- Demonstrations

- New in TRITON Management Server

TRITON Management Server

- Audit Log

- Single sign-on

- Two-factor authentication
  - Uses a client SSL certificate as a key

- Support for SQL Server non standard port
  - Port selectable during TRITON Infrastructure installation
  - Port selectable during Log Server installation
  - Port can also be changed after installation
  - Must use standard port when using SQL Server Express 2008 R2

- **Support for SQL Server SSL encryption**
  - **Microsoft SQL Server must be pre-configured**
  - **Caveats:**
    - **Log Database connections is slower**
    - **Cannot use BCP (a data insertion method)**
    - **Cannot run TRITON - Web Security console on the appliance**
      - **Dashboard and reporting data are not available**
- **Hardware**
  - **Windows Server 2008 R2 64 bit is required**
  - **Windows Server 2003 is no longer supported**
    - **Except for Data Security**

- **New in Websense Web Security**

Websense Web Security

- **Enhanced Web Security Dashboard**
  - **Tools to fight advanced persistent threats**
  - **Severity-based alerting on suspicious Internet activity**
    - **Incident table like the one in the full Data Security Server (DSS)**
  - **New health alerts for transparent identification and logging**
- **Policy Exceptions**
  - **Replaces Unfiltered URLs for permitting clients to blocked categories**
  - **More intuitive and easier to use**
  - **Exceptions can be created for:**
    - **Single client, list of specific clients, or all clients in all roles**

Websense Web Security

- Enhanced file type blocking
  - If not initially blocked, Content Gateway determines its true file type
- Extended information on block page
  - ACEInsight link
  - Real-time category, Static category, Category set by
- Log Server configuration now integrated into TRITON – Web Security console
- Enhanced Log Database configuration
  - Growth rates and sizing chart
  - Internet Browse Time (IBT) option for Investigative Reports
  - Trend data retention policy

Websense Web Security

- Enhanced DC Agent configuration
  - View list of domain controllers queried by DC Agents
  - Configure domain discovery
- Time-based (stateful) support for multiple Filtering Services
  - Share timing information for:
    - Quota
    - Confirm
    - Password Override
    - Account Override
  - Websense State Server (new service)
  - Only State Server service per filtering domain

Websense Web Security

- Support for YouTube
  - Provides access to videos even when YouTube content is blocked
  - You must be enrolled and obtain a school account code
- Integration with third-party SIEM solutions
  - Requires installing a Multiplexer service for each Policy Server
  - Multiplexer passes data, from Filtering Service, to Log Server and SIEM product
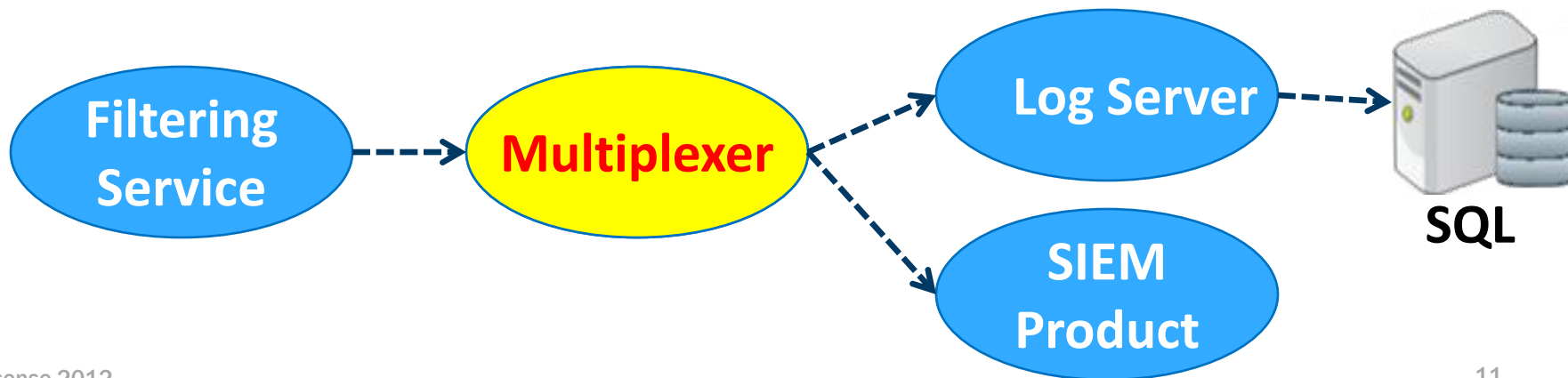
- **Filtering of IPv6 addresses (software and appliance)**
  - Network Agent or Content Gateway required
  - IPv4 must still be available for machines hosting:
    - Websense components
   - Directory Services
    - DNS

- **New in V-Series Appliance**

V-Series Appliance

- **Hotfix management**
  - All-inclusive resource for managing hotfixes
- **Permanently disable Network Agent**
  - Redistributes CPU and memory resources
  - CAUTION: Restoring requires appliance re-image
- **SNMP alerting enhancements**
  - Time-based thresholds
  - Generate event-cleared alerts

V-Series Appliance

- **Admin credentials required when 'physically' accessing the appliance Command Line Interface**

- **Support for IPv6**

  - **Disabled on appliance by default**

  - **Explicit proxy is supported**

    - **Transparent proxy is not supported**

  - **Dual IP stack on C, N, P1, P2, and E1/E2 interfaces (if configured)**

  - **V-Series appliance communicates with Websense components via IPv4**

- **New in Websense Content Gateway**

Websense Content Gateway
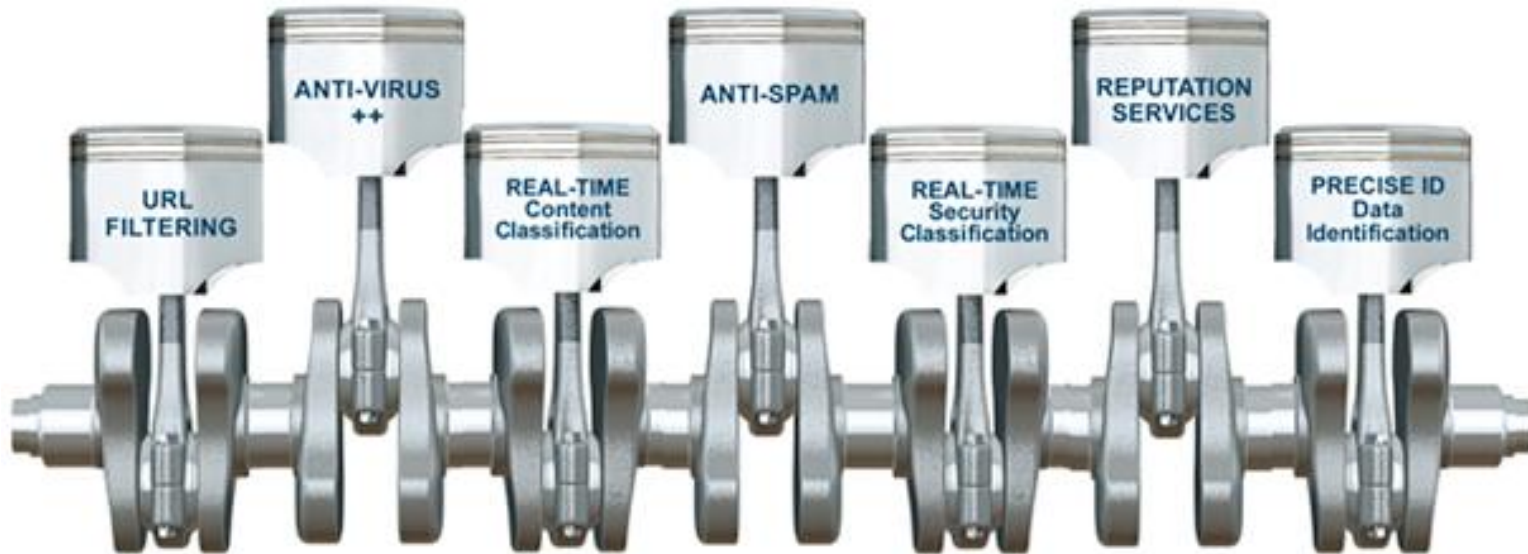
- Updated user interface, look and feel
  - Consistent look with other TRITON modules
- SSL Manager enhancements
  - SSL Manager uses the same certificate as Content Gateway Manager
  - SSL Decryption bypass options
    - Client bypass by IP address and IP address range
    - Destination bypass by hostname, IP address, and IP address range
  - SSL certificate verification engine (CVE)
    - Updated trusted certificate store
    - Stronger hash function
    - Server Name Indication (SNI) connection retry
    - Fewer "Unknown revocation state" errors

Websense Content Gateway

- **Client connection limits**
    - A client concurrent connection limit (default = 1000)
    - A client connection rate limit (default = 100 per second)
    - Set proxy to close connection requests above the connection limit, alarm on the condition, or both
    - Exempt clients from limits (by IP address)
- **New scanning option:**
    - Content delay handling
        - Delivers a portion of the buffered content before scanning completes
        - Reduced wait-time for non-blocked traffic

Websense Content Gateway

- **Additional real-time analytics**
  - **Malicious IFrame detection**
  - **Suspicious PDF detection**
  - **Outbound data theft protection**
  - **Dynamic file type updates**
- **SIEM integration**
- **FIPS (Federal Information Processing Standard) 140-2 mode**
  - **Not reversible without a complete reinstall of Content Gateway**
- **Enhancements to WCCP v2 support**
  - **Content Gateway can accept traffic from multiple subnets**
  - **Full support for GRE encapsulation on the return path**
  - **You need to specify a Virtual IP (in the WCG) for each router that performs WCCP**

Websense Content Gateway

- **Support for sites that use custom header**
  - YouTube for Schools
  - Google Apps for Business
- **Integrated SOCKS server on V-Series appliances**
- **Limitations for Content Gateway IPv6 support**
  - Only explicit proxy deployments
    - ARM does not support IPv6 addresses
  - Parent proxy in a chain cannot be IPv6
  - IP spoofing is not supported
  - SOCKS proxy is not supported

- **Introducing Mobile Security**

Mobile Security

- **The TRITON console links to the Mobile Security portal**
    - The portal is a cloud-based console used to manage threat protection and data loss prevention for mobile devices
    - You filtering and email polices

- **Mobile Security provides:**
    - **Mobil Device Management (MDM)**
        - **Password enforcement, remote lock, wipe, encryption, and more**
    - **Identifies malicious applications**
    - **Email data loss protection**
    - **Reporting**
    - **And more...**

Additional Information

- **Websense TRITON console– [Release Notes](#) or [Help](#)**

- **Websense Web Security– [Release Notes](#) or [Help](#)**

- **Websense Content Gateway– [Release Notes](#) or [Help](#)**

- **Websense V-Series Appliances– [Release Notes](#) or [Help](#)**

- **Websense TRITON Mobile Security– [Web](#) or [Data Sheet](#)**

- **Deployment and Installation Center ([web](#) or [PDF](#))**

- **[What is the lookup precedence for Policy Exceptions?](#)**

- **[Allow content hosted by YouTube for Schools](#)**

- **[Web Security Default Ports](#)**

- **[Upgrade Center](#)**

websense®

Webinar

Update

Title: **Upgrading to Websense Web Security v7.7**

Date: **August 15th, 2012**

Time: **8:30 A.M. PDT (GMT -8)**

How to register:
http://www.websense.com/content/SupportWebinars.aspx

websense®

- To find Websense classes offered by Authorized Training Partners in your area, visit: http://www.websense.com/findaclass

- Websense Training Partners offer classes online and onsite at your location.

- For more information, please send email to: readiness@websense.com

Websense Customer Training

Designed for:
- ▷ System administrators
- ▷ Network engineers
- ▷ Other members of your organization as appropriate

Training locations:
All training is conducted at Authorized Training Centers (ATCs). Each ATC has information on costs, course schedules, and types of classes (in-person, virtual, or computer-based).

websense®
Authorized Training Center