Cisco E-mail and Web Security News

SEC3 / L2

Hrvoje Dogan, Consulting Systems Engineer, Security
Prosíme, ptejte se nás

- Twitter  www.twitter.com/CiscoCZ
- Talk2cisco  www.talk2cisco.cz/dotazy
- SMS  721 994 600
Program

- E-mail Security Appliance: AsyncOS 7.6
- Cloud E-mail: European Data Centers
- Web Security Appliance: AsyncOS 7.5
- ScanSafe: Extending the Cloud to the premises
AsyncOS for E-mail 7.6 Release

Now Available At An ESA Near You!
Aria Program Feature List

**IPv6**
- IPv6 / Dual Stack Support
- On Box Reputation Engine

**Hotlist**
- Subject Header Edit in Content Filters
- DKIM Enhancements
- Rate Limiting on Mail-From
- TLS Settings Based on Mail-From Address

**DLP**
- DLP Quarantine and Continue
- RSA Enterprise Manager Phase 1
- RSA Fingerprinting
- Ability to Limit Access to DLP Data to Some Users/Roles
Rate Limiting by Mail-From
Business Use Cases

Rate-Limiting Per Envelope Sender can control:

- Automated mail or runaway applications
- Outbound user mail per company policy
- Outbound spam

Use this in conjunction with Outbreak Filters to help customers combat phishing attacks where the stolen credentials are being used to turn them into a spam cannon.
Web UI Configuration

- Mail Policies -> Mail Flow Policies -> Default Policy Parameters
Logging and Alert

• A message is logged every time a recipient is rejected due to Rate Limiting:

Tue Oct 11 21:38:30 2011 Info: MID 133 To: <rogandhi@cisco.com> From: <rogandhi@cisco.com> Rejected by Rate Limiting per Envelope Sender

• An Info level System alert is generated when a recipient is rejected due to Rate Limiting:

System is rate limiting Envelope Sender <rogandhi@cisco.com> due to high volume of messages

Version: 0.0.0-000
Serial Number: 000C29FE5E7D-0000000
Timestamp: 11 Oct 2011 21:38:30 -0700
TLS Settings by Mail-From
Business Case

- Enforce TLS on incoming email from a select set of domains.

Today, customers have the ability to send emails encrypted and to force them to go encrypted with an option to fall back to envelope encryption if TLS is unavailable.

They do not have the ability to force senders to use TLS encryption.

This feature closes that gap and allows customers to force business partners to use TLS to send them emails.
**Enforcing TLS via Mail Flow Policy**

<table>
<thead>
<tr>
<th>Security Features</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam Detection:</td>
<td>On</td>
</tr>
<tr>
<td>Virus Protection:</td>
<td>On</td>
</tr>
<tr>
<td>Encryption and Authentication:</td>
<td>TLS:</td>
</tr>
<tr>
<td>SMTP Authentication:</td>
<td>Off</td>
</tr>
<tr>
<td>If Both TLS and SMTP Authentication are enabled:</td>
<td>Require TLS To Offer SMTP Authentication</td>
</tr>
<tr>
<td>Domain Key/DKIM Signing:</td>
<td>On</td>
</tr>
<tr>
<td>DKIM Verification:</td>
<td>On</td>
</tr>
</tbody>
</table>

**TLS is Mandatory for Address List:**

A security certificate/key has not been uploaded to a listener. (See Network > Certificates.) Enabling TLS is required to use "Demo" certificate/key for listeners.

**Business Partners:**

None
Example Conversation

EHLO rsa.com

250-esa.eng
250-8BITMIME
250-SIZE 20971520
250 STARTTLS

MAIL FROM: <employee@rsa.com>

530 #5.7.0 This sender must issue a STARTTLS command first
Logs

Tue Oct 4 01:43:18 2011 TLS is required for employee@rsa.com on ICID 1234 but remote host did not initiate it
On-Box Reputation Engine
Business Use Cases

Removes SBRS code from base MTA:

- Allows for a separate engine to do the work – reducing memory footprint and allowing for separate updates
- Allows for re-use of the data – not just at initial SMTP connection anymore
- Is critical to delivering IPv6 reputation
- Does not change the behavior of how the box gets SBRS information via the web

This changes licensing requirements: Anti-Spam license must be present on-box!
Subject Header Edit in Content Filters
Business Case

Administrators want to Manage, via the GUI, the removal of subject line flags used to mark emails for special handling such as emails that are manually marked for:

• Encryption
• Bypassing Encryption
• Bypassing DLP policies
• Other special handling as desired

This also allows for the appending/prepending of text to a header and for the insertion of a new header.
What Has Changed?

The Content Filter Action of Add Header:

**Add Header**

 Inserts a header and value pair into the message before delivering. To replace a header, use this action after Strip Header.

Header Name: ____________

Header Value (optional): ____________

Is now Add/Edit Header:

**Add/Edit Header**

Inserts a header and value pair into the message or modifies an existing header and value pair before delivering.

Header Name: ____________

New Header Name or Existing Header

- Specify Value for New Header (optional):
  ____________

- Prepend to the Value of Existing Header:
  ____________

- Append to the Value of Existing Header:
  ____________

- Search & Replace from the Value of Existing Header:
  Search for: ____________
  Replace with: ____________

Leave blank to remove searched text from value.

(*') accepts regular expression
Editing Headers
Add/Edit Content Filter Conditions

Scenario: Customer marks emails with the subject line tag [Secure] to manually flag it for encryption but does NOT want the tag to go out on the email.

First, create an outgoing Content Filter to look for the key word [Secure]
Next, set a Content Filter Action to Edit the Subject header and remove the [Secure] tag.

Simply leave the "Replace with" field empty to remove the searched text.

Note: The header name MUST be specified
DKIM Enhancements
Business Case

Users want to Manage:

• DKIM Verification Profiles
• Customization of DKIM Signing Profiles
• Disabling DKIM Signing for system generated messages
• Disabling DKIM Signing using Content and Message Filters
DKIM Verification Profiles

New DKIM Verification Profile screen:

Add DKIM Verification Profiles

Outbound DKIM Verification

Profile Name: test_verification_profile

Smallest Key to be Accepted: 512 Bits

Largest Key to be Accepted: 2048 Bits

Minimum Number of Signatures in the Message to Verify:

Key Query Timeout Limit:

Limit to Tolerate Wall Clock Asynchronization Between Sender and Verifier:

Use a Body Length Parameter:

SMTP Action for Temporary Failure:

SMTP Action for Permanent Failure:

Submit
DKIM Signing Profiles Granularity

Add DKIM Signing Profile with optional tags:

<table>
<thead>
<tr>
<th>Outbound Domain Key Signing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name:</td>
</tr>
<tr>
<td>Domain Key Type:</td>
</tr>
<tr>
<td>Domain Name:</td>
</tr>
<tr>
<td>Selector:</td>
</tr>
</tbody>
</table>

Canonicalization:
- Headers:
  - Simple
- Body:
  - Simple

Sign Key: [cisco_key]

Headers to Sign:
- All
- Standard
- Additional Headers: (optional)

Body Length to Sign:
- Whole Body Implied
- Whole Body Auto-determined
- Signed Content is Possible

Include Tags to Signature:
- ""Tag (Identity of the user or agent)
- "a" Tag (Identity of the User or Agent)
- "q" Tag (A colon-separated list of query methods, used to retrieve the public key)
- "ct" Tag (Creation time stamp of the signature)
- "z" Tag (Signature expiration time)
- Expiration Time of Signature: 315360000 seconds
- "V" Tag (Vertical-bar-separated list of header fields present when the message was signed)
DKIM Signing Profiles Granularity

Test results for DKIM Signing Profile with optional tags:

<table>
<thead>
<tr>
<th>DKIM Signing</th>
<th>Result of DKIM processing: Message signed (profile: cisco)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DKIM Verification</td>
<td>Result of DKIM Verification processing: no signature</td>
</tr>
<tr>
<td>SPF Verification</td>
<td>Result of SPF Verification processing: SPF verification not enabled in this listener's HAT</td>
</tr>
<tr>
<td>Message Delivery (matched on policy DEFAULT)</td>
<td></td>
</tr>
<tr>
<td>Final Envelope Sender:</td>
<td><a href="mailto:vantonev@cisco.com">vantonev@cisco.com</a></td>
</tr>
<tr>
<td>Final Recipients:</td>
<td><a href="mailto:vantonevych@lohika.com">vantonevych@lohika.com</a></td>
</tr>
</tbody>
</table>
| Final Message:                                    | DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=cisco.com; s=s; t=1314279740; x=1345815740; h=from:to:subject:message-id:date; bh=yZQl8wjj80fZ4kC/oraNCAG1mZJv5w/hlvyFy+t6A=; b=KvmmMv6/8ECax8mNdusly/B5d5cF8G7pODvaem79hH7zDepyVe6K3vTZdG/7le0O5s0VnCHMj9y1sH2EOwHw3E2HjfyRD8wQ0KgeSuuBRf0d2Mq+Ta0AGJTv71r4bi3P0K1xQhjbmLVL8rkqC9NOYGb7QcEv3CZVgOqbP=/3=; Authentication-Results: outgoing_listener; dkim=neutral (message not signed) header.i=none Message-Id: <le5e3f@outgoing_listener> Date: 25 Aug 2011 13:42:20 +0000 Received: from localhost by rhino.eng; 25 Aug 2011 13:42:20 +0000 From: vantonev@cisco.com To: vantonevych@lohika.com Subject: Test DKIM Signing Profile

Hello.
Content Filters
Skip DKIM Signing

Add Bypass DKIM Signing Content Filter Action:

![Add Action Menu]

- Bypass DKIM Signing
- Quarantine
- Encrypt on Delivery
- Strip Attachment by Content
- Strip Attachment by File Info
- Add Disclaimer Text
- Bypass Outbreak Filter Scanning

**Bypass DKIM Signing**

Bypass DKIM Signing for this message.

Click OK to add this rule. There are no configurable options for this rule.
IPv6 Support
Business Case

• IPv6 is around the corner
  IPv4 address Issues
  National IPv6 Strategies
  Increasing application support – OS, Content, Web.

• IPv6 Email-based threats are just starting to emerge
  Cisco only player to invest in Reputation-based blocking

• Stepwise Implementation Plan
  Hosted
  SBRS efficacy for IPv6 will improve as the traffic increases.
Example Use Cases

• Sending/Receiving Mail over IPv6
  SMTP and most of the Email related features in ESA support IPv6 now.

• Seamless Dual Stack Support
  An interface can have both IPv4/IPv6 address. So the same Listener and associated policies work without any change.
  Configurable delivery preferences (IPv4/IPv6).

• Basic IPv6 Management support
  Http/Ssh supported over IPv6 as well.
### IPv6 Enabled Features

<table>
<thead>
<tr>
<th>HAT</th>
<th>RAT</th>
<th>Routes</th>
<th>Filters</th>
<th>Destination Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace</td>
<td>NIC Pairing</td>
<td>Outbreak Filters</td>
<td>TLS</td>
<td>SMTP Routes</td>
</tr>
<tr>
<td>SMTP Callahead</td>
<td>Admin ACL</td>
<td>Tracking</td>
<td>Reporting</td>
<td>Http(s)/Ssh</td>
</tr>
</tbody>
</table>

SBRS will be supported for IPv6 addresses as well. In addition, we are enhancing the Reputation mechanism (It uses the SMTP HELO domain along with IP address) to increase efficacy.
# Feature Overview

## Not Supported Features* – Planned in next Phase

<table>
<thead>
<tr>
<th>Feature</th>
<th>ESQ</th>
<th>Communication with SMA</th>
<th>DNS</th>
<th>LDAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clustering</td>
<td>ESQ</td>
<td>Communication with SMA</td>
<td>DNS</td>
<td>LDAP</td>
</tr>
<tr>
<td>SNMP</td>
<td>FTP</td>
<td>Updates/Upgrades</td>
<td>Sending Alerts</td>
<td>Remote Access</td>
</tr>
</tbody>
</table>

* These features currently will work over IPv4 only.
Configuration Interface Settings

IP Interface Settings

Name: 
Ethernet Port: Data 1
IPv4 Address / Netmask: 
(example: 10.1.1.0/24)
IPv6 Address / Prefix: 
(example: 2001:0d08:65a3::0000:82e:0370:7334/64)
Hostname: 
HTTPS Certificate: System Default

Services:

- FTP (Applicable only for IPv4 addresses.)
- Telnet
  If you enable telnet on this interface, network access restrictions will not be applied for Telnet connections originating from IPv6 hosts.
- SSH
- HTTP
- HTTPS
- Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)
- Spam Quarantine HTTP
- Spam Quarantine HTTPS

Network Interfaces and IP Addresses

Add IP Interface...

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Hostname</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>dual</td>
<td>1.1.1.1/24, 2001::3/64</td>
<td>asd.com</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>10.76.69.133/24</td>
<td>test.com</td>
<td></td>
</tr>
<tr>
<td>v4</td>
<td>3.3.3.3/24</td>
<td>v4.com</td>
<td></td>
</tr>
</tbody>
</table>
## Configuration

### Destination Controls

![Destination Controls](image)

- **Destination:**[Blank]
- **IP Address Preference:**
  - Default (IPv6 Preferred)
  - IPv6 Preferred
  - IPv6 Required
  - IPv4 Preferred
- **Limits:**
  - Use Default (500)
  - Maximum of 500 (between 1 and 1,000)
- **IPv4 Required:**
  - Use Default (50)
  - Maximum of 50 (between 1 and 1,000)
- **Per Connection:**
  - Use Default (No Limit)
  - Maximum of 0 per 60 minutes
  - Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60
- **Apply limits:**
  - Per Destination:
    - Entire Domain
    - Each Mail Exchanger (MX Record) IP address
  - Per ESA hostname:
    - System Wide
    - Each Virtual Gateway
    - (recommended if Virtual Gateways are in use)
- **TLS Support:**
  - Default (None)
# Configuration

## Routing

### IPv4 Gateway (Default Router) and Static Routes

<table>
<thead>
<tr>
<th>Route Name</th>
<th>Destination</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>external</td>
<td>1.1.1.1</td>
<td>192.168.1.0</td>
</tr>
<tr>
<td>Default Route</td>
<td>All Other Destinations</td>
<td>10.76.69.1</td>
</tr>
</tbody>
</table>

### IPv6 Gateway (Default Router) and Static Routes

<table>
<thead>
<tr>
<th>Route Name</th>
<th>Destination</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal</td>
<td>2001::1/64</td>
<td>2001::</td>
</tr>
<tr>
<td>Default Route</td>
<td>All Other Destinations</td>
<td></td>
</tr>
</tbody>
</table>
Reporting/Tracking

On-box and off-box Reporting/Tracking will show IPv6 addresses along with IPv4.

Incoming Mail Details

<table>
<thead>
<tr>
<th>Sender IP Address</th>
<th>Hostname</th>
<th>Total Attempted</th>
<th>Stopped by Reputation Filtering</th>
<th>Stopped as Invalid Recipients</th>
<th>Spam Detected</th>
<th>Virus Detected</th>
<th>Stopped by Content Filter</th>
<th>Total Threat</th>
<th>Marketing</th>
<th>Clean</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8:85a3:8a2e:370:7336</td>
<td>...nd.soma.ironport.com</td>
<td>467</td>
<td>0</td>
<td>0</td>
<td>98</td>
<td>0</td>
<td>0</td>
<td>98</td>
<td>66</td>
<td>303</td>
</tr>
<tr>
<td>204.15.82.110</td>
<td>...nd.soma.ironport.com</td>
<td>409</td>
<td>0</td>
<td>0</td>
<td>97</td>
<td>0</td>
<td>0</td>
<td>97</td>
<td>57</td>
<td>255</td>
</tr>
<tr>
<td>2001:db8:85a3:8a2e:370:7336</td>
<td>...nd.soma.ironport.com</td>
<td>407</td>
<td>0</td>
<td>0</td>
<td>103</td>
<td>0</td>
<td>0</td>
<td>103</td>
<td>51</td>
<td>253</td>
</tr>
<tr>
<td>204.15.82.126</td>
<td>...mx.soma.ironport.com</td>
<td>406</td>
<td>0</td>
<td>0</td>
<td>115</td>
<td>0</td>
<td>0</td>
<td>115</td>
<td>46</td>
<td>247</td>
</tr>
<tr>
<td>204.15.82.101</td>
<td>...nd.soma.ironport.com</td>
<td>375</td>
<td>0</td>
<td>0</td>
<td>96</td>
<td>0</td>
<td>0</td>
<td>96</td>
<td>35</td>
<td>245</td>
</tr>
<tr>
<td>2001:db8:85a3:8a2e:370:7336</td>
<td>...mx.soma.ironport.com</td>
<td>329</td>
<td>0</td>
<td>0</td>
<td>52</td>
<td>0</td>
<td>0</td>
<td>52</td>
<td>32</td>
<td>245</td>
</tr>
<tr>
<td>2001:db8:85a3:5555:5555:8a2e:1370:7221</td>
<td>...nd.soma.ironport.com</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>40</td>
<td>17</td>
<td>243</td>
</tr>
</tbody>
</table>

Top Senders by Clean Messages

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8:85a3:8a2e:370:7336</td>
<td>403</td>
</tr>
<tr>
<td>204.15.82.110</td>
<td>255</td>
</tr>
<tr>
<td>2001:db8:85a3:8a2e:370:7336</td>
<td>253</td>
</tr>
<tr>
<td>204.15.82.126</td>
<td>247</td>
</tr>
<tr>
<td>204.15.82.101</td>
<td>245</td>
</tr>
<tr>
<td>2001:db8:85a3:8a2e:370:7336</td>
<td>243</td>
</tr>
<tr>
<td>2001:db8:85a3:8a2e:370:7336</td>
<td>231</td>
</tr>
<tr>
<td>204.15.82.104</td>
<td>231</td>
</tr>
<tr>
<td>204.15.82.102</td>
<td>228</td>
</tr>
</tbody>
</table>

Results

Displaying 1 — 20 of over 250 items.

1. 11 Apr 2011 13:23:49 (GMT -07:00)  MID: 114259988  SBRBS: -8.3
   HOST: Corvette (2001:db8:85a3:0000:0000:8a2e:0370:7334)
   SENDER: j.bowen_pm@students.oamk.fi
   RECIPIENT: offers@synfs.com
   SUBJECT: (no subject)
   LAST STATE: Message 114259988 on incoming connection (ICID 15840563) added recipient: offers...

2. 11 Apr 2011 13:23:37 (GMT -07:00)  MID: 114259986  SBRBS: -8.3
   HOST: Corvette (2001:db8:85a3:0000:0000:8a2e:0370:7334)
   SENDER: anuvmjat@synfs.com
   RECIPIENT: anuvmjat@synfs.com
   SUBJECT: anuvmjat@synfs.com Rolex.com For You -39%
   LAST STATE: Message 114259987 to anuvmjat@synfs.com received remote SMTP response 'sent'.
Update on New Cloud Data Centers
Virtualization in Action

European Data Centers

In-Continent Redundancy

Dedicated Instances
Update on New Cloud Data Centers

Business Cases

The new data centers will help with customers who

• Want in-theater data centers
• Are worried about the Patriot Act / Privacy Laws
AsyncOS for Web 7.5 Release

New Features of the WSA
Roadmap Update
Matterhorn – Back to Basics

- Invest in core product functionality
- Focus on value, ease of use, deployability
Roadmap Update
Some Big Rocks

- Adaptive Scanning
- URL Category Parity
- Transparent User ID for Active Directory
- AsyncOS Reversion
- Refactored Native FTP Proxy
## Roadmap Update

### Lots of Pebbles

<table>
<thead>
<tr>
<th>Re-brand as Cisco</th>
<th>Session-based EUA</th>
<th>RADIUS admin authorization</th>
<th>Fewer WCCP resets</th>
</tr>
</thead>
<tbody>
<tr>
<td>L4TM Reporting and Tracking</td>
<td>Accept IP in XFF header</td>
<td>AsyncOS Upgrade Notification</td>
<td>Roll logs at time of day</td>
</tr>
<tr>
<td>New default EUN pages</td>
<td>More watchdogs</td>
<td>Syslog push for access logs</td>
<td>Show side effect of policy deploy</td>
</tr>
<tr>
<td>Save EUA across proxy restart</td>
<td>64-bit SNMP counters</td>
<td>Feature Key network path</td>
<td>User preferences in UI</td>
</tr>
</tbody>
</table>
Roadmap Update
Beta Feedback

Beta Customers: 17

Customer Feedback:

"These boxes are literally getting better and better. This is a testament to you guys."

"Matterhorn is very cool. The features you have added are really usable, and both Chris and I are really excited about using in production."

"The SMA is fine and it is intuitive."

"I've been in the business for 12 years and this is my favorite box. It is very intuitive."
Adaptive Scanning

What Is It?

• New content scanning logic
• Intelligently selects scanners based on content type and risk profile
• Better efficacy: targeted scanning
• CPU savings – better performance
• Easy configuration
Adaptive Scanning
How Does It Work?

• Scanner(s) selected for targeted content, rather than using all scanners for all content

• Scanner selected based on:
  Reputation
  Content type
  AV scanner(s) available or licensed
  AV scanner catch rate for the content type
  AV scanner scanning cost

• Scanning queue: higher risk content scanned first

• Low risk content scanned when box is at low load, to confirm verdicts

• Can be enabled on a per-policy basis
### Adaptive Scanning

**Global Configuration**

- Enable Reputation Filtering by checking the box. This will configure the Global Access Policy to use Web Reputation Filtering & Adaptive Scanning.

<table>
<thead>
<tr>
<th>Security Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Policy Default Action:</strong></td>
<td>Monitor all traffic, Block all traffic. If block all traffic is selected, the Global Access Policy will be initially configured to block all proxied protocols (HTTP, HTTPS, FTP over HTTP, and native FTP).</td>
</tr>
<tr>
<td><strong>L4 Traffic Monitor:</strong></td>
<td>Action for Suspect Malware Addresses: Monitor only, Block</td>
</tr>
<tr>
<td><strong>Acceptable Use Controls:</strong></td>
<td>Enable: The Global Access Policy will be initially configured to monitor all pre-defined categories. Acceptable Use Controls Service: Cisco IronPort URL Filters, Cisco IronPort Web Usage Controls</td>
</tr>
<tr>
<td><strong>Reputation Filtering:</strong></td>
<td>Enable: The Global Access Policy will be initially configured to use Web Reputation Filtering and Adaptive Scanning.</td>
</tr>
<tr>
<td><strong>Malware and Spyware Scanning:</strong></td>
<td>Enable Webroot, Enable McAfee, Enable Sophos. The Global Access Policy and Outbound Malware Scanning Policy will be initially configured to apply...</td>
</tr>
</tbody>
</table>
Adaptive Scanning
Per-Policy Basis

• Enable Reputation Filtering for the policy. This will configure the access policy to use Web Reputation Filtering & Adaptive Scanning.

• To disable Web Reputation & Adaptive Scanning for a particular policy, uncheck the Reputation Filtering box. You will then have to select your DVS Anti-Malware settings in the boxes below it.
New URL Categories
What Are The New Categories?

• Better, more accurate categories
  New categories
  Categories merged, split, or removed

• Category updates no longer tied to WSA releases
  Flexibility to adapt to changing Internet landscape
  Updates as needed, likely no more than every 6 months

• Cloud integration: same categories as ScanSafe
New URL Categories
How Changes Are Implemented

• Categories pushed out to WSA during updates

• When update occurs, summary of category changes & policy changes emailed to admin

• Automatic conversion of policy to new categories after update
  
  Policies generally retained – most changes map directly to old categories

  Least restrictive policy wins

• Reports & tracking show category at time of transaction
Transparent User Identification
Workflow

1. User logs in against Active Directory

2. AD pushes domain, username and IP address to the AD agent. Save IP-User database to disk periodically

3. User tries to access the Internet via WSA

4. If the IP-User mapping is not in the local database, query AD agent for the user of the new IP address

5. Add returned mapping to local database

6. Allow access to the Internet if policy permits

WSA

AD Agent

Active Directory
Transparent User Identification
Realm Configuration

- Network > Authentication > Add/Edit Realm
New Application Signatures

Maintaining High Efficacy: Ongoing Updates to Existing Signatures
Additional Centralized Reporting Options

- Recommended for 25K+ users
- SMA-equalivalent reports
- Group-based reports
- Sold and supported by Cisco
ScanSafe: Web Security In The Cloud

Security & Policy

Infrastructure

Deployment & Integration
Security & Policy
New Search Ahead

- Supports Google Instant
- Supports Bing, Yahoo
- Works with encrypted search
- Faster
Application Visibility & Control

Identical to the WSA AVC engine except:

**Bandwidth control**
- Added in follow-on phase
- Roadmap Q4 CY’12

**YouTube Site Control ratings**
- AVC implementation will not support site control ratings
- ScanSafe has the ability to enforce SafeSearch in search engines but this does not extend to YouTube

Beta: Feb 4th 2012
FCS: Apr 5th 2012
Security Enhancements

Outbreak Intelligence™
• New versions of scanlets released
  - PDF
  - HTML
  - Exe
  - Java

Reputation & Databases
• Categories now identical between ScanSafe and WSA (Matterhorn)
• Integrate WebRep into OI (Jul 2012)
• Merge databases (Oct 2012)

Cisco anti-malware
• Developing next-generation of scanning technology
Enhanced Portal Authentication

- A global password policy enforcement
- Password strength checker
- Provides granular access audit log
- Data will include: IP address, time, username, company of user, status
- Any failed login attempts will be presented with a CAPTCHA challenge
Reports: User Audit

User: John Doe

Session-based reporting
Detailed browsing history
User forensics

<table>
<thead>
<tr>
<th>Session</th>
<th>Host</th>
<th>Category</th>
<th>Rule Action</th>
<th>First Seen</th>
<th>Last Seen</th>
<th>Browse Time (Min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Sessions - Total duration 1754 minutes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session 1 - Total duration 3 minutes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>electradl.player.bbc.co.uk</td>
<td>Search Engines and Portals</td>
<td>allow</td>
<td>05-12-2011 11:51</td>
<td>05-12-2011 11:53</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td><a href="http://www.bbc.co.uk">www.bbc.co.uk</a></td>
<td>Streaming Video</td>
<td>allow</td>
<td>05-12-2011 11:51</td>
<td>05-12-2011 11:53</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>clients5.google.com</td>
<td>Search Engines and Portals</td>
<td>allow</td>
<td>05-12-2011 11:53</td>
<td>05-12-2011 11:53</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td><a href="http://www.bbc.co.uk">www.bbc.co.uk</a></td>
<td>Streaming Audio</td>
<td>allow</td>
<td>05-12-2011 11:53</td>
<td>05-12-2011 11:53</td>
<td>1</td>
</tr>
<tr>
<td>Session 2 - Total duration 13 minutes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>electradl.player.bbc.co.uk</td>
<td>Search Engines and Portals</td>
<td>allow</td>
<td>05-12-2011 12:01</td>
<td>05-12-2011 12:01</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>stats.bbc.co.uk</td>
<td>Infrastructure and Content Delivery</td>
<td>allow</td>
<td>05-12-2011 12:01</td>
<td>05-12-2011 12:13</td>
<td>13</td>
</tr>
<tr>
<td>Session 3 - Total duration 4 minutes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>sqm.microsoft.com</td>
<td>Computers and Internet</td>
<td>allow</td>
<td>05-12-2011 12:43</td>
<td>05-12-2011 12:43</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>cfr.microsoft.com</td>
<td>Computers and Internet</td>
<td>allow</td>
<td>05-12-2011 12:46</td>
<td>05-12-2011 12:46</td>
<td>1</td>
</tr>
</tbody>
</table>
Infrastructure
Datacenters: Execution to Plan
What’s Next

• New datacenters: Mexico & Dubai

• Exploring business case for new regions: Russia, Spain & Italy

• Local towers with Service Providers
  • Open to the possibility for large/strategic partners
  • Clarity on implementation details
ScanSafe IPv6 Roadmap

Phase I: mid-CY 2012
Phase II: end-CY 2012
Deployment & Integration
ScanSafe Secure Mobility
With AnyConnect 3.0

- Security & policy even when off-network and off-VPN
- Connects to closest tower
- Seamless integration with AnyConnect interface

Internet Traffic

VPN
Internal Traffic (optional)

AnyConnect Web Security
Cloud-enabled Branch

Web Traffic Split Tunnel

Branch User → ISR G2 → Backhaul VPN → Head Office

Internet
ISR ScanSafe Details

Supported Platforms

- **Available in IOS** (universal) images w/security feature set (SEC/K9) licenses
- Support for 880, 890, 19XX, 29XX and 39XX/E ISR G2 platforms
- Released in 15.2(1)T

Functionality

- In-line transparent redirection (not WCCP)
- Supports redirection of HTTP/HTTPS traffic with authentication
- Exceptions/whitelisting at router (by hostname, User-agent, URI regex)
- Transparent integration with LDAP and Active Directory
- No need for client or agent software on endpoint
- No proxy settings for the web browsers will need to be changed
- Policy management & reporting configured using ScanCenter portal

<table>
<thead>
<tr>
<th>Releases</th>
<th>Phase 1</th>
<th>Phase 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timeline</strong></td>
<td>By Jan 15, 2012</td>
<td>1H 2012</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>No Auth HTTP Auth Proxy</td>
<td>No Auth HTTP Auth Proxy HTTP Basic Auth</td>
</tr>
<tr>
<td><strong>NTLM Support</strong></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Release Vehicle</strong></td>
<td>Engineering Supported</td>
<td>TAC Supported</td>
</tr>
</tbody>
</table>
## ISR G2 Sizing Guideline

### ScanSafe Users Supported per ISR G2 Platform

<table>
<thead>
<tr>
<th>Phase</th>
<th>3945E</th>
<th>3925E</th>
<th>3945</th>
<th>3925</th>
<th>2951</th>
<th>2921</th>
<th>2911</th>
<th>2901</th>
<th>1941</th>
<th>1921</th>
<th>891</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Auth</td>
<td>5000</td>
<td>5000</td>
<td>1200</td>
<td>900</td>
<td>600</td>
<td>500</td>
<td>400</td>
<td>350</td>
<td>350</td>
<td>300</td>
<td>120</td>
</tr>
<tr>
<td>Web Proxy</td>
<td>1200</td>
<td>1200</td>
<td>1200</td>
<td>900</td>
<td>600</td>
<td>500</td>
<td>400</td>
<td>350</td>
<td>350</td>
<td>300</td>
<td>120</td>
</tr>
<tr>
<td>HTTP Basic</td>
<td>1200</td>
<td>1200</td>
<td>1200</td>
<td>900</td>
<td>600</td>
<td>500</td>
<td>400</td>
<td>350</td>
<td>350</td>
<td>300</td>
<td>120</td>
</tr>
<tr>
<td>NTLM</td>
<td>1200</td>
<td>1200</td>
<td>1200</td>
<td>900</td>
<td>600</td>
<td>500</td>
<td>400</td>
<td>350</td>
<td>350</td>
<td>300</td>
<td>120</td>
</tr>
</tbody>
</table>
Zero Footprint Deployment: Easy ID

- Browser-based
- No hardware or software installation
- Authentication in the cloud

Supports:
- HTTP / HTTPS traffic with granularity
- All browsers on all platforms
- Supports Microsoft AD, LDAP-based directories

Internet

Data-center

Security & Policy

Identification & Authentication

P.I.M.

EasyID

Directory

Connector

User

© 2011 Cisco and/or its affiliates. All rights reserved.
Transaction Flow - Top Level

Customer

Browser

Customer LDAP

HTTP to Web Site

Not authenticated

User logs in

HTTP to Web Site

ScanSafe

Tower

Authenticate rule applied

Authenticated

Browser redirected to Captive Portal

Captive Portal queries with LDAPS

User identity established with LDAP attributes

Browser redirected to Web Site

HTTP to Web Site

Policy applied based on LDAP Attribute

Internet

Web Site

Policy applied based on LDAP Attribute

User logs in

Browser redirected to Captive Portal

Captive Portal queries with LDAPS

User identity established with LDAP attributes

Browser redirected to Web Site

HTTP to Web Site

Authenticated

Internet

Web Site
Otázky a odpovědi

• Twitter  www.twitter.com/CiscoCZ
• Talk2Cisco  www.talk2cisco.cz/dotazy
• SMS  721 994 600

• Zveřejníme Vás na Ptali jste se… v sále LEO
  1.den 17:45 – 18:30
  2.den 16:30 – 17:00
Prosíme, ohodnoťte tuto přednášku.