Cisco Hybrid Web Security

Any Where, Any Device, Any Time –

Martin Briand
Security Escalation VSE – Global Virtual Engineering
June 2016
Our Agenda

• Security Today: Trends and Disruptions
• Your Security Needs
• **Cisco Hybrid Web Security**
• Roadmaps
Better Security Visibility

Securing the Mobile Enterprise

Protect Against Advanced Malware

Improve Results with Security Services

Harden and Segment the Network

Security as a Network Driver
Our goal is to make security less complex by providing a best of breed portfolio that’s deeply integrated and delivers solutions that are superb individually, but vastly more powerful when used together.
Why Web Security?

19.7 Billion
Total Threat Blocks

Daily

7.2 Trillion
Yearly

82 Thousand Virus Blocks
181 Million Spyware Blocks
818 Million Web Blocks

Daily Web Breakdown

This is information gathered by Talos, Cisco’s Security Intelligence and Research Group.
Web Security Is More Important Than Ever Before

- The web is a popular attack vector for criminals
- Without proper control, your own users can put your business at risk
- Increased cloud adoption creates blind spots
Web Security Customer Requirements

Large amounts of https traffic

Detailed web and HR reporting

Need for deep inspection and control including AVC

Corporate network

Proxy

Roaming user
# Web Security Deployment Choices & Tradeoffs:

## On-premise Web Security

- Headquarters
- Remote Sites
- Locations without a Cloud Offering

## Cloud Web Security

- Mobile Users
- Locations with Cloud Offerings

### Ideal Deployment

<table>
<thead>
<tr>
<th>On-premise Web Security</th>
<th>Cloud Web Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Benefits</strong></td>
<td><strong>Concerns</strong></td>
</tr>
<tr>
<td>• Increased Performance</td>
<td>• Cost</td>
</tr>
<tr>
<td>• Localized manageability &amp; control</td>
<td>• Maintenance &amp; Upgrades</td>
</tr>
<tr>
<td><strong>Concerns</strong></td>
<td><strong>Cisco's Solution</strong></td>
</tr>
<tr>
<td>• Cost</td>
<td>• Web Security Appliance (WSA)</td>
</tr>
<tr>
<td>• Maintenance &amp; Upgrades</td>
<td>• Web Security Virtual Appliance (vWSA)</td>
</tr>
<tr>
<td>• Regulations</td>
<td>• Security Management Appliance (SMA)</td>
</tr>
<tr>
<td>• Bandwidth required to access cloud</td>
<td>• Cloud Web Security (CWS)</td>
</tr>
</tbody>
</table>

---

Cisco’s Solution:
- Web Security Appliance (WSA)
- Web Security Virtual Appliance (vWSA)
- Security Management Appliance (SMA)
Challenge: Web Security is Portable

Mobile  Coffee shop  Corporate  Home  Airport
Cisco’s Hybrid Web Security – Any Where / Any Device / Any Time
Extending Protection Beyond the Network

Key Benefits
- Save network bandwidth
- Improve user experience
- Defend against malware
- Protect your investment

Use Case 1
- Remote Sites
- Mobile User
- CWS Browser
- WWW

Use Case 2
- Remote Sites
- Mobile User
- CWS Browser
- WWW

WAN
VPN
Unified Policy Configuration & Reporting

Unified Reporting
- Roaming user
- HQ
- WSA
- Web Security Reporting Application

Unified Policies
- Roaming user
- HQ
- WSA
- Cloud Web Security Graphical User Interface
Cisco Web Security

Before
- Web Filtering
- Web Reputation
- Application Visibility and Control

During
- Webpage
- Anti-Malware
- File Reputation

After
- Outbreak Intelligence
- File Sandboxing
- DLP Integration
- File Retrospection
- Cognitive Threat Analytics

Key:
- CWS Only
- WSA/WSAv Only
- Hybrid
- Allow
- Warn
- Block
- Partial Block

Client Authentication Methods
- ASA
- WSA
- Explicit/PAC
- ISR G2
- ISR 4K
- AnyConnect

Traffic Redirection Methods
- WCCP
- Load Balancer
- Explicit/PAC
- PBR
- AnyConnect

Reporting
- Management
- Log Extraction

Campus Office
- Branch Office
- Roaming User
- BYOD User
Cisco Hybrid Web Security: Manage all policies from a single location – the Cloud

Master your environment
Powerful centralized management and reporting provides admins the capability to orchestrate and manage policies across all devices

Control your business
Manage all your devices both on and off-premises

Simplify the process
Manage everything through a single location

Identify
Gain visibility into web usage across devices and services

Analyze
Gather insight into the data and applications your company uses and the threats you face

Control
Set and enforce consistent policies across offices and remote users

Advanced Malware Protection
Acceptable Use policies
Web Filtering policies
Threat Score acceptance levels
Access permissions

HQ
Branch
Roaming Laptops
Today:

Cisco Hybrid Use Case – Phase 1
Customer wants to add On-Prem WSA for areas that do not have a local tower or political reasons to have an on-prem device. However, policy still controlled by cloud.

Step 1:
On-Prem device must be configured locally by an admin or technician. WSA is configured in Hybrid Mode, network configurations to allow pairing with Scancenter and Cisco Adv Reporting Application as well as any other network settings will be configured locally first.

Step 2:
Scancenter sees new on-prem WSA then is able to configure or push current policy to those users.

Step 3:
Cisco Adv Reporting application is able to report on both CWS and on-prem WSA.
One comprehensive bundle

Web security bundle: HYB-WEB-SEC

Features

CWS
- Cloud Web Security Essentials
  - Web usage controls
  - Malware scanning
  - Secure mobility

WSA
- Web Security Premium
  - Web usage controls
  - Malware scanning
  - Web security reporting application (optional)

Benefits

- Flexible Solution
  Purchase Cisco Web security for cloud or on premises

- Choice of License
  Order new or renewal via GPL

- Custom Mix
  Shift between CWS & WSA during contract or renewal

- Unified Price
  Get consistent pricing for WSA or CWS seats
  - GPL offering – Brazil and Indian Datacenters for CWS not available
  - Offer available for distribution sell through, not for stocking (software bundle)
Licensing Example

Web Security reporting bundle
- Support an initial mix of 30k WSA and 13k CWS
- Communicate changes in user mix to ipss-salesoperations@cisco.com

Optional add-ons
- Support 43k total users through the Web Security Reporting App
- Extend CWS log extraction to 13k users (i.e. same as those allocated to CWS)
## Hybrid Web Security Roadmap

<table>
<thead>
<tr>
<th>1H CY15</th>
<th>2H CY15 (June 2015)</th>
<th>1H CY16 (January 2016)</th>
<th>2H CY16 (Fall 2016)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Log Extraction from CWS</td>
<td>• Unified reporting on premise</td>
<td>• Unified Policy management</td>
<td>• Centralized Cloud Reporting</td>
</tr>
<tr>
<td>• CWS Policy Backup and Restore</td>
<td></td>
<td>• New Customer User Interface</td>
<td>• Extended Health Monitoring &amp; Device Management</td>
</tr>
</tbody>
</table>

Disclaimer: Many of the products and features described herein remain in varying stages of development and will be offered on a when-and-if-available basis. This roadmap is subject to change at the sole discretion of Cisco, and Cisco will have no liability for delay in the delivery or failure to deliver any of the products or features set forth in this document.
Cisco Web Security: The Protection You Require...Period!

- Cisco Web Security Appliance (WSA)
- Cisco Cloud Web Security (CWS)