Cisco ISR with Cisco Cloud Web Security Connector

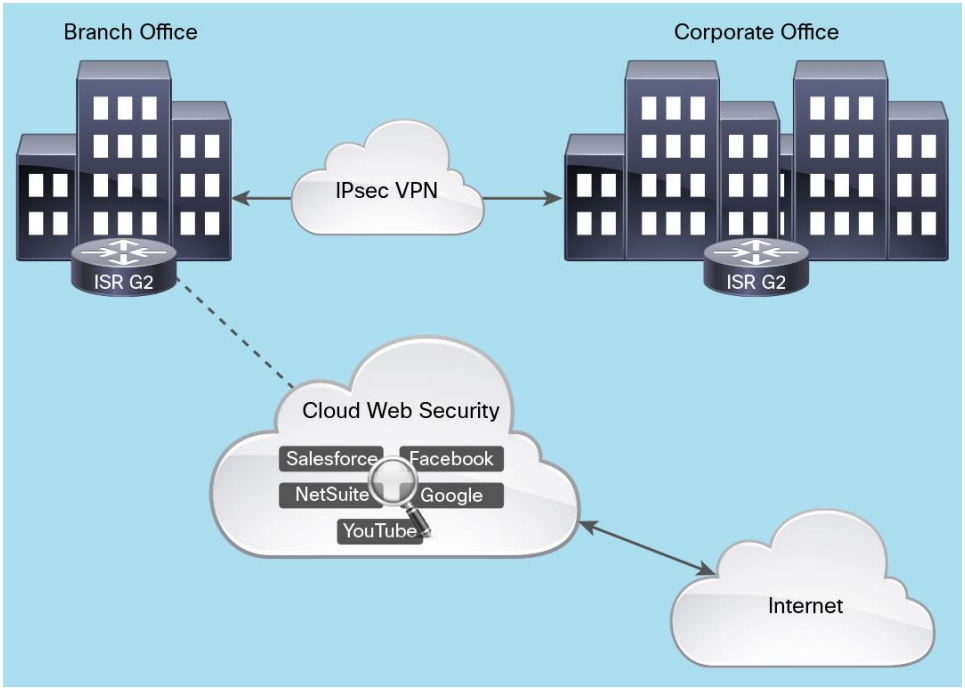
Now you can extend the numerous security services of the Cisco® Integrated Services Router (ISR) family with a simple, cost-effective, on-demand web security solution that requires no additional hardware.

Product Overview

The Cisco Cloud Web Security Connector extends ISR firewall, intrusion prevention, VPN, and other security features. You can deploy market-leading web security quickly and easily and provide highly secure local Internet access for all sites and users, saving bandwidth, money, and resources.

With Cisco ISR with Cloud Web Security Connector, branch offices can intelligently redirect web traffic to the cloud to enforce detailed security and control policy over dynamic Web 2.0 content (Figure 1). The solution helps protect branch office users from threats such as Trojans, back doors, rogue scanners, viruses, and worms. The connector is available in the Cisco Security SEC-K9 license bundle.

Figure 1. Typical Cisco ISR with Cloud Web Security Deployment



Features and Benefits

Cisco ISR with Cloud Web Security Connector:

- Works independently but can also be used with Cisco IOS® Software-based security solutions such as the Zone-Based Policy Firewall, Intrusion Prevention System (IPS), and Secure Sockets Layer (SSL) and IPsec VPNs
- Supports detailed policies for web usage and security
- Can drastically reduce an organization's on-premises hardware footprint, pushing all high-resource-intensive tasks (such as content analysis, report storage, and generation) to the cloud
- Provides zero-day threat protection powered by Cisco Outbreak Intelligence, which uses dynamic reputation- and behavior-based analysis
- Blocks at least 25 percent more malware than traditional signature-based security solutions
- Eliminates the need to backhaul Internet traffic from branch offices, so offices can access the web directly, without losing control of or visibility into web usage

The Cisco ISR integrates with directory services such as Active Directory, so policies can be defined and enforced right down to the individual user. Cisco ISR with Cloud Web Security Connector offers web content filtering and zero-day malware protection. Organizations can build a detailed global policy for all web traffic, including SSL-encrypted communications. Security policy can be based on categories, content, file types, schedules, and quotas. Integrated outbound policy helps ensure that confidential data, such as customer details or credit card numbers, does not leave the network.

Cisco ISR with Cloud Web Security Connector analyzes every piece of web content accessed, including HTML, images, scripts, and Flash content. Each piece is analyzed using artificial-intelligence-based "scanlets" to build a detailed view of each web request and the associated security risk. All resource-intensive operations, from content analysis to global reporting, are cloud based. As a result, the web security functionality does not affect the performance of the other ISR services.

Why Choose Cisco ISR with Cisco Cloud Web Security Connector?

- **Lower total cost of ownership:** The connector helps you avoid the costs associated with the deployment and maintenance of on-premises software and hardware.
- **Leading security and peace of mind:** Real-time cloud-based scanning blocks malware and inappropriate content before it reaches the network.
- **Scalability and availability:** Our global network processes high volumes of web content at high speeds, everywhere, for a true global solution that is always available.
- **Integration with other Cisco security products:** Cisco ISR Web Security with Cloud Web Security integrates with Cisco AnyConnect® to offer a web security solution for users both on and off the network.
- **Consistent, unified policy:** An acceptable use policy (AUP) can be applied to all users regardless of location, simplifying management.
- **Predictable operational expenses:** Clients can plan capacity and budget.

Supported Features

- **User and group authentication** that sends information to Cloud Web Security towers. Separate web filtering policies are implemented for each group
- **User authentication methods,** including HTTP basic (Lightweight Directory Access Protocol [LDAP]), WebAuth (RADIUS, LDAP, and local), and Windows NT LAN Manager (NTLM) v1 and v2 (LDAP)
- **Active authentication** (which validates credentials) and **passive authentication** (which does not)
- Browser-based **authentication bypass**
- IP-based, host-based, and user agent-based **whitelisting**
- **Traffic redirection** that sends all HTTP and HTTPS traffic (destined for the Internet) to the Cloud Web Security towers for potential web filtering and malware scanning

Centralized Management and Reporting

Cisco ISR with Cloud Web Security Connector is managed through ScanCenter, an intuitive web-based interface, which integrates all management and reporting capabilities (Figure 2). A global web security policy can be created and enforced across the organization, even down to the group or user level, and any edits to the policy are rolled out in real time. ScanCenter offers overview data, ongoing trending reports, and forensic audits (Figures 3 and 4).

Figure 2. Example of ScanCenter Reporting Output

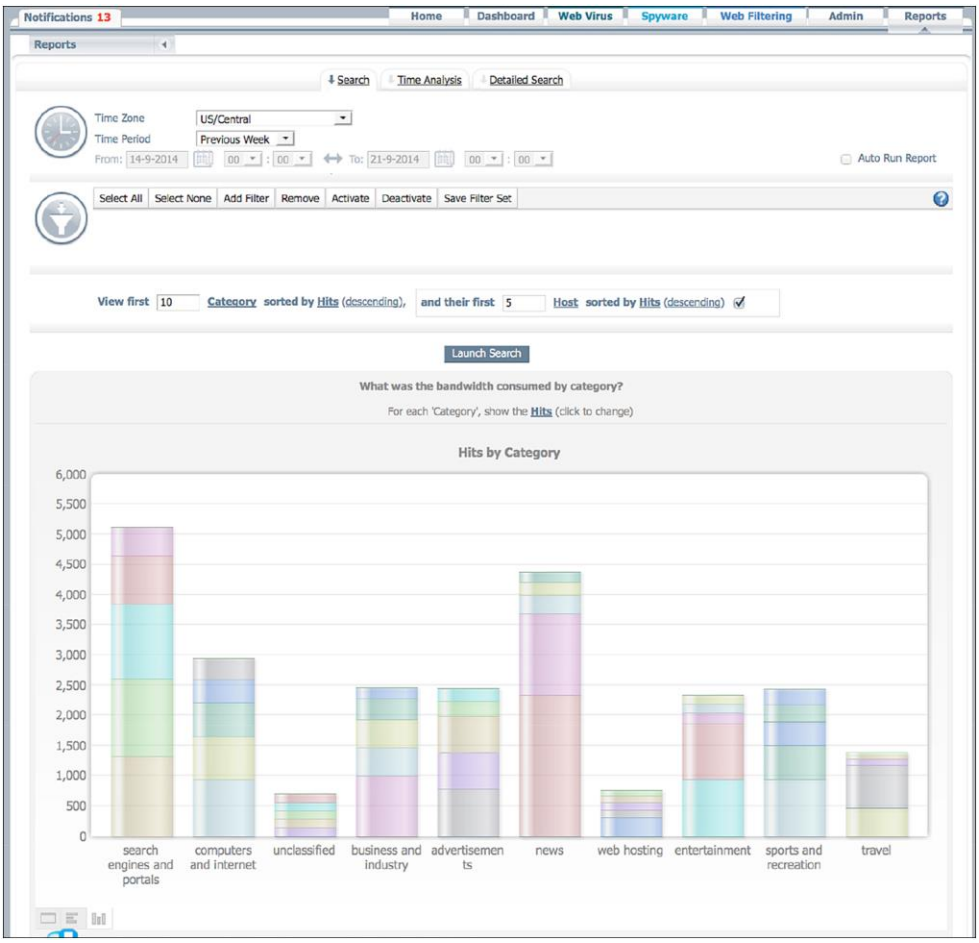


Figure 3. ScanCenter Web Filtering Reporting Output

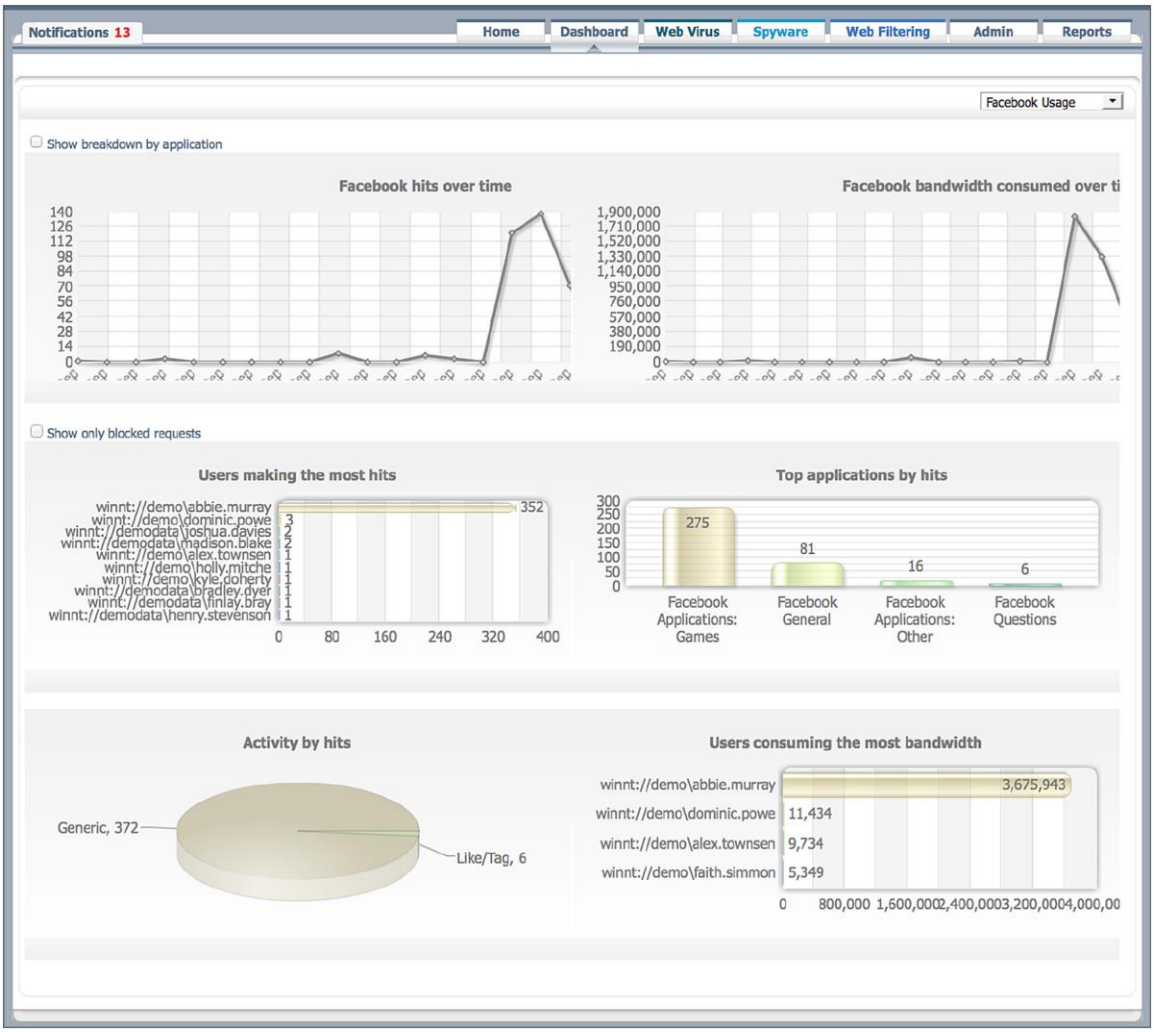
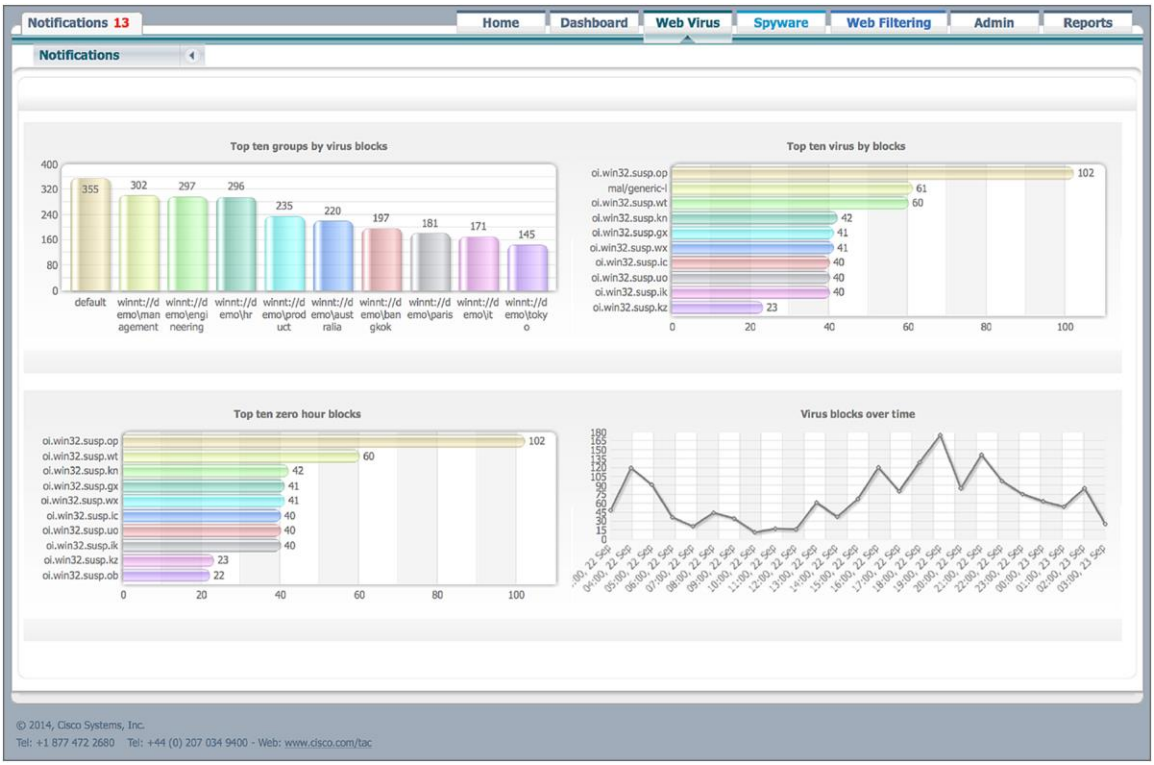


Figure 4. ScanCenter Web Filtering Reporting Output Showing Blocked Viruses



Cisco Security Manager

Cisco Security Manager is an enterprise-class management application that is designed to configure firewall, VPN, and IPS security services on Cisco network and security devices. Its unified interface can be used to activate the Cisco ISR with Cloud Web Security feature in Cisco IOS Software in large-scale deployments.

Supported Platforms

Table 1 lists the router platforms that support Cloud Web Security.

Table 1. Platform Support for Cloud Web Security

Router Series	Supported Models
Cisco 800 Series Routers	http://www.cisco.com/c/dam/en/us/td/docs/routers/access/800/software/compatibility/800Compatibility.XLSX
Cisco 1900 Series Integrated Services Routers	Cisco 1905, 1921, 1941, 1941W
Cisco 2900 Series Integrated Services Routers	Cisco 2901, 2911, 2921 and 2951
Cisco 3900 Series Integrated Services Routers	Cisco 3925, 3925E, 3945, 3945E

Performance

Table 2 displays the average throughput and connections per second for Cisco Cloud Web Security on supported platforms. Cisco ISR Generation 2 routers can run a maximum of 32,000 concurrent sessions, regardless of the platform type.

Table 2. Cloud Web Security Average Performance Numbers on Supported ISR Models

Feature	Performance	Cisco ISR Model										
		891	1921	1941	2901	2911	2921	2951	3925	3925E	3945	3945E
Cloud Web Security	Throughput in Mbps	101	268	293	286	310	387	592	801	982	916	992
	Connections per second	73	195	212	207	225	280	429	580	711	663	718
Cloud Web Security plus Network Address Translation (NAT)	Throughput in Mbps	69	120	132	129	140	173	218	302	917	330	971
	Connections per second	50	87	95	93	101	125	158	218	664	239	702
Cloud Web Security plus Zone-Based Firewall	Throughput in Mbps	72	136	149	145	157	195	250	342	957	387	974
	Connections per second	52	98	108	105	114	141	181	247	692	280	704
Cloud Web Security plus Zone-Based Firewall plus NAT	Throughput in Mbps	43	87	95	94	102	124	139	192	611	215	751
	Connections per second	31	63	69	68	74	90	101	139	442	156	543
Cloud Web Security plus IPS	Throughput in Mbps	44	59	64	62	68	85	102	142	802	164	949
	Connections per second	32	42	46	45	49	61	74	103	580	119	687
Cloud Web Security plus Zone-Based Firewall plus IPS	Throughput in Mbps	35	53	57	55	60	74	87	120	615	137	764
	Connections per second	25	38	41	40	43	53	63	87	445	99	552
Cloud Web Security plus NAT plus Zone-Based Firewall plus IPS	Throughput in Mbps	28	43	47	46	50	60	70	98	430	110	535
	Connections per second	20	31	34	33	36	44	51	71	311	80	387

Test Methodology

- All the test results were obtained using a local simulated tower setup in the lab, and not with a real Cloud Web Security tower.
- Throughput and connections per second were measured with the maximum CPU on each platform without any drop rate.
- Tests were run with each connection fetching 16,000 objects, which means that every HTTP get request is answered by 16,000 objects, which is the average seen across Cloud Web Security deployments.
- Tests were done to with a maximum of 0.0001 percent transaction failures.
- Tests were run with the maximum memory on each platform.

The actual Internet traffic profile may vary based on usage, but we strongly recommend that customers adhere to the sizing guidelines provided in Table 3

Table 3 displays the number of users that each Cisco ISR G2 platform can support. These numbers represent only the Cloud Web Security Connector service enabled on the Cisco ISR G2 router. These numbers do not represent the Cisco ISR G2 router running other software services operating together with the connector.

Table 3. Scaling for the Supported Cloud Web Security Platforms (in Number of Users)

Cisco ISR G2 Router Model		Authentication (NTLM, HTTP Basic, Web Proxy)	No Authentication
800		120	120
1921		300	300
1941		350	350
2901		350	350
2911		500	500
2951		600	600
3925		900	900
3925E		1,200	5,000
3945		1,200	1,200
3945E		1,200	5,000

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For More Information

For more information about Cisco Integrated Services Routers and Cisco ISR Web Security with Cloud Web Security visit:

- Cisco ISR G2 platform: http://www.cisco.com/go/isrg2
- Cisco Cloud Web Security: http://www.cisco.com/c/en/us/products/security/router-security/isr_web_security.html
- Cloud Web Security Solution Guide: http://www.cisco.com/c/dam/en/us/products/collateral/security/router-security/cws-solution-guide.pdf
- Cloud Web Security Design Guide: http://www.cisco.com/c/dam/en/us/products/collateral/security/router-security/cws-design-guide.pdf
- Troubleshooting Guide: http://www.cisco.com/c/dam/en/us/products/collateral/security/router-security/cws-troubleshooting.pdf

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-655324-06 08/16