Cisco ISR Web Security with Cisco ScanSafe

Product Description

Q. What is Cisco ISR Web Security with Cisco ScanSafe?

A. The Cisco® Integrated Services Router Generation 2 (ISR G2) Family delivers numerous security services, including firewall, intrusion prevention, and VPN. These security capabilities have been extended with Cisco ISR Web Security with Cisco ScanSafe, a simple, cost-effective, on-demand web security solution that requires no additional hardware. Organizations can deploy and enable market-leading web security quickly and easily, and can enable secure local Internet access for all sites and users, saving bandwidth, money, and resources.

Cisco ISR Web Security with Cisco ScanSafe 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 impact the performance of the other ISR G2 services.

Q. What ISR models support Cisco ISR Web Security with Cisco ScanSafe?

A. All Cisco ISR G2 platforms support Cisco ISR Web Security with Cisco ScanSafe (Table 1).

Table 1.   Platforms and Products That Support Cisco IRS Web Security with Cisco ScanSafe

Platforms	Products That Support Cisco ISR Web Security with Cisco ScanSafe
Cisco 800 Series Routers	Cisco 819, 881, 881W, 886, 886W, 886VA, 887V, 887W, 887VA, 887VA-M, 887VA-M, 888E, 888E, 888, 888W, 891, 891W, 892, 892W Integrated Services Routers
Cisco 1900 Series Integrated Services Routers	Cisco 1941 and 1941W Integrated Services Routers
Cisco 2900 Series Integrated Services Routers	Cisco 2901, 2911, 2921 and 2951 Integrated Services Routers
Cisco 3900 Series Integrated Services Routers	Cisco 3925, 3925E, 3945, and 3945E Integrated Services Routers

Q. How does this differ from Cisco IOS Content Filtering?

A. Cisco ISR Web Security with Cisco ScanSafe goes beyond the simple URL filtering capabilities offered by Cisco IOS® Content Filtering. In addition to using a more granular URL database, Cisco ISR Web Security with Cisco ScanSafe incorporates dynamic website categorization, bidirectional content control, and effective protection from zero-day malware threats using a combination of web reputation and real-time content analysis.

Q. How is this different from anti-virus software?

A. While the Cisco ScanSafe service does incorporate multiple anti-virus engines, this is only the first line of protection to block known threats. Once web content has been passed as "safe" by the anti-virus engines, it is passed through our Outbreak Intelligence engine, which, because it is based on artificial-intelligence-driven content analysis and virtualized code emulation, requires no signature updates in order to detect and block zero-day threats. This is the true security value of the service.

Q. Does Cisco ScanSafe block more malware than anti-virus engines?

A. Yes. We have seen that more than 25 percent of all malware blocks made by Cisco ISR Web Security with Cisco ScanSafe are zero-day blocks that would have evaded traditional anti-virus engines.

Q. Does Cisco ScanSafe support control over web application platforms such as Facebook and LinkedIn?

A. Although customers can control these web applications using Cisco ISR Web Security with Cisco ScanSafe, we plan to enhance this capability to make the policy creation and management of these controls simpler and more dynamic. The goal is to take the workload off the administrator and support application controls dynamically using Cisco Security Intelligence Operations (SIO).

Q. Can Cisco ScanSafe control content that is leaving the network?

A. Yes, there are controls in place to enable the management of what content can leave the network via the web.

Q. Where is policy and security enforced?

A. All enforcement takes place within the Cisco ScanSafe cloud. All web traffic is forwarded directly to the Cisco ScanSafe infrastructure, where both policy and security analysis takes place. This ensures that this resource-intensive approach to web security has no impact on the performance of the ISR G2 platform.

Q. What reporting capabilities are available?

A. The Cisco ScanSafe service offers global, real-time visibility into web trends and usage for all users through Web Intelligence Reporting (WIRe). All storage and report generation takes place in the cloud, returning reports in seconds as opposed to hours, which is the norm for traditional systems.

With around 100 attributes stored for every web request, and all reporting data available for access by administrators, WIRe enables reporting flexibility with granularity down to the user level.

Q. Does Cisco ISR Web Security with Cisco ScanSafe protection extend to roaming users?

A. Yes. As a cloud service, in addition to protecting on-premises users utilizing the Cisco ISR platform, this protection extends to all mobile users who operate outside the network. Integration with the Cisco AnyConnect™ Secure Mobility Client ensures that all web traffic is passed directly to the nearest Cisco ScanSafe data center where all policy and security is applied.

Q. How does this enable a cost-effective distributed WAN strategy?

A. Implementing Cisco ISR Web Security with Cisco ScanSafe can enable a dramatic reduction in backhaul traffic by allowing remote sites to access the Internet directly rather than through a central site. This reduction of load on expensive Multiprotocol Label Switching (MPLS) circuits saves money and also frees up bandwidth for internal applications.

Q. How is the ISR deployed?

A. The Cisco ISR is deployed in-line, providing transparent authentication for users.

Q. Does the ISR G2 integrate with directory services?

A. Yes, the Cisco ISR G2 integrates with directory services, such as Microsoft Active Directory, to enable policies to be defined and enforced right down to the individual user. Cisco ISR Web Security with Cisco ScanSafe offers web content filtering and zero-day malware protection and allows organizations to build a granular global policy for all web traffic, including Secure Sockets Layer (SSL)-encrypted communications.

Q. Does Cisco ISR Web Security with Cisco ScanSafe work with the IOS Security features on the Cisco ISR G2?

A. Yes. Cisco ISR Web Security can work independently or can be used simultaneously with Cisco IOS Software-based security solutions such as Cisco IOS Firewall, Cisco IOS IPS, and Cisco IOS SSL and IPSec VPNs.

Ordering

Q. What products are required for Cisco ISR Web Security with Cisco ScanSafe?

A. There are three components required:

- Cisco ISR G2 platform as listed in Table 1
- Security SEC K9 license bundle for Cisco ISR
- Cisco ScanSafe Web Security service subscription

Q. How is the Cisco ScanSafe service priced?

A. The Cisco ScanSafe Web Security service, as a subscription, is priced per user, per month. The price per month varies on pricing bands based on the number of users and the subscription term (12, 24, or 36 months).

The number of users is the total number of users across the entire organization, not per site.

The pricing calculation is as follows:

(Number of users) * (Number of months) * (Cost per month) = Total for subscription

Q. How is the user count calculated?

A. The user count is the total number of Internet users within the global organization as a whole. A user is defined as an identity that exists within authentication directories. Licensing is not defined per device. There is no per site license subscription.

Printed in USA

C67-662214-01   09/11