



8 Essentials of Internet Security

Today's Internet is about much more than simple web browsing, which means total Internet security requires much more than basic firewalls and content filtering. To keep your organization safe and productive, you need tools that provide precise, fine-grained control over the infinite variety of Internet content that enters your organization. You have to dynamically prioritize and manage both content and bandwidth. And of course, you need intelligent security solutions that can adapt to evolving techniques and emerging threats.

So what does it take to build an Internet security solution with all of these capabilities and characteristics? Here are 8 essential steps to consider as you work towards a complete, capable Internet security framework.

1 Deploy an inline, deep packet inspection device

An inline device allows you to see all your Internet traffic, and deep-packet inspection makes it possible to identify and control traffic as it enters your organization. Traditional web proxies and firewalls are easy to bypass and simply can't provide the same degree of flexible, fine-grained protection.

2 Implement Layer 7 application controls

Today, 50 percent of a typical organization's bandwidth is consumed by applications, which means you need the ability to prioritize and control that traffic. With the right Layer 7 application controls in place, you can reserve bandwidth for critical applications, limit bandwidth for non-critical applications and eliminate potentially harmful application traffic.

3 Take advantage of dynamic content shaping

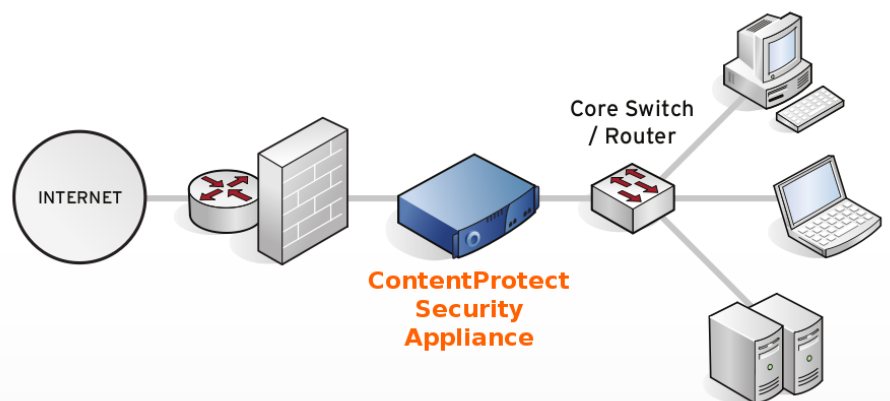
Outdated content filters give you the option of either allowing or denying access to specific Web sites and online content. Dynamic content shaping moves past this inflexible on/off approach by allowing you to intelligently categorize and prioritize Internet traffic. This keeps critical information fast and available, while still allowing users to access recreational content when extra bandwidth is available.

4 Provide dynamic, real-time anonymous proxy detection

Anonymous proxies make it relatively easy to bypass most Internet security devices. You need a solution that can dynamically detect and control these dangerous filter bypass methods in real time.

► The ContentProtect Security Appliance is a secure web gateway device that offers you a fast, affordable way to meet the 8 Essentials of Internet Security.

► An effective Internet security device inspects, categorizes and prioritizes web traffic, so you can take control of your connection.





Find out how ContentWatch can help you meet the 8 Essentials of Internet Security quickly and affordably.

Visit www.contentwatch.com or call 866.765.7233 to learn more, schedule a live demo or sign up for a free evaluation.

- 5 Provide dynamic, real-time URL filtering**
Many traditional content filters still rely on URL databases to categorize Web sites. Unfortunately, millions of new Web sites are created every day, which makes any database-only approach insufficient and incomplete. Effective Internet security devices must combine traditional URL databases with dynamic, real-time filtering capabilities that make it possible to categorize potentially dangerous websites on the fly.
- 6 Ensure full HTTPS traffic inspections**
HTTPS connections prevent most traditional content filters from inspecting content inside encrypted sessions, which essentially renders them useless. As a result, your security solution needs the ability to decrypt, inspect and then re-encrypt HTTPS sessions.
- 7 Implement Web-based malware blocking**
Any effective Internet security solution must be able to block all attempts to download malware—even when those threats are contained within HTTPS traffic or come from trusted sources.
- 8 Ensure accurate correlation between events and users**
To keep your Internet connection healthy and safe, you need total visibility into what users are doing online. This includes detailed information about which online applications they’re using, how much bandwidth they’re consuming, exactly which threats they’re being exposed to and how individual actions are affecting the overall connection. By correlating specific issues, you can diagnose problems accurately and find effective solutions.

▶ Linking raw Internet usage data to specific users makes it easy to accurately diagnose and correct problems quickly.

