SOPHOS

Security made simple.

Endpoint web control overview guide

Sophos Web Appliance
Sophos UTM (version 9.2 or later)
Sophos Enterprise Console
Sophos Endpoint Security and Control

Document date: April 2016

Contents

1 Endpoint web control

Sophos Web or UTM appliances can perform filtering for URLs and file types at the network gateway. Sophos Enterprise Console allows you to extend some of this same capability to endpoints via Sophos Endpoint Security and Control, filtering 14 essential site categories on user machines.

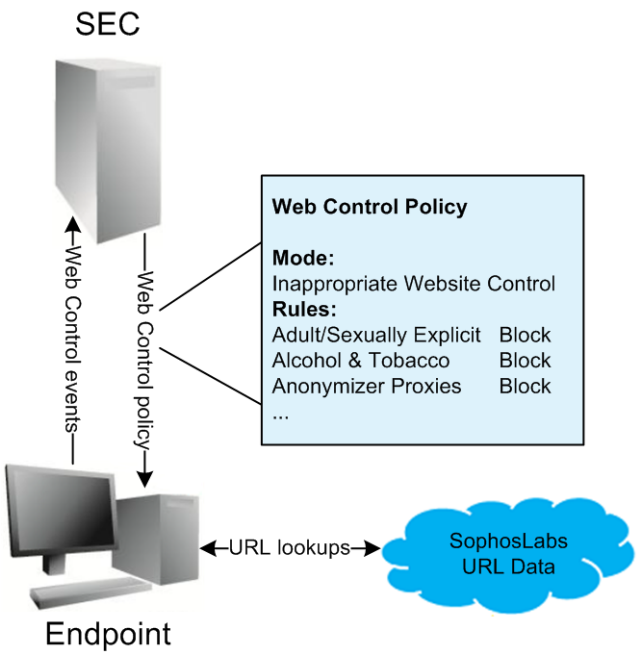
By combining a Sophos appliance with Sophos Enterprise Console, however, your organization can take advantage of features that both products have to offer. Once you have configured them to work together, you can apply a Full Web Control policy (with more than 50 site categories) to each user machine by way of Endpoint Security and Control.

Endpoints then receive policy updates and send web activity reports to the appliance, and send web events to Enterprise Console.

Enterprise Console can enable endpoint web control using three different methods:

- Enterprise Console only
- Enterprise Console and Web Appliance
- Enterprise Console and UTM

2 Enterprise Console only



Even without a Web Appliance or Management Appliance, Enterprise Console offers basic web filtering. When a web control policy is configured and enabled solely through Enterprise Console,

rules for 14 essential site categories are applied for each user through Sophos Endpoint Security and Control. The policy, defined on Enterprise Console as “Inappropriate Website Control,” is published to users. Users’ web activity data is sent back to Enterprise Console, where the results are displayed as “web events.”

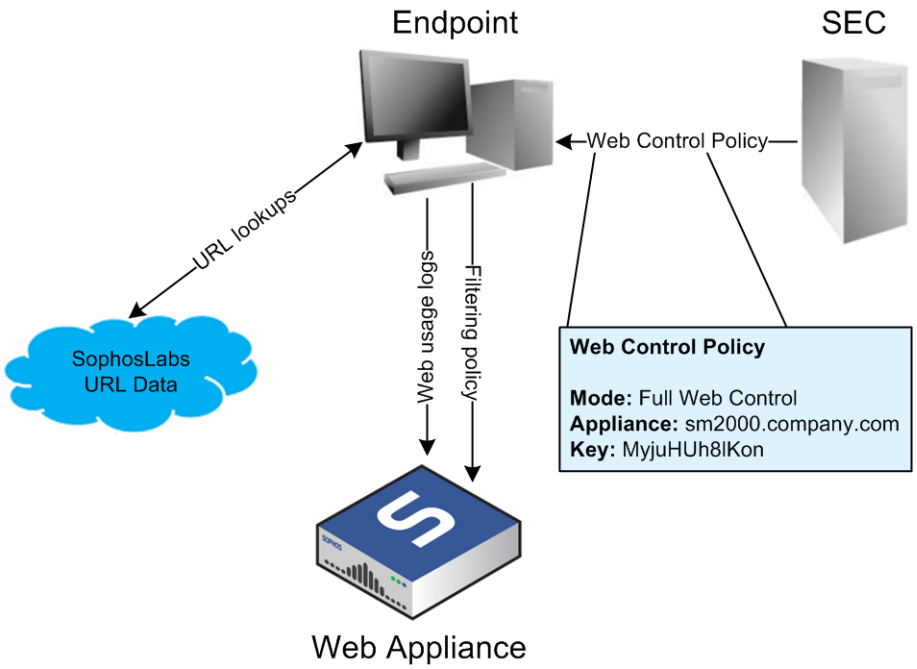
The live URL-filtering feature dynamically checks URLs through SXL queries to SophosLabs, obtaining the latest threat information. SXL is the infrastructure that Sophos uses to submit real-time, DNS-based queries to SophosLabs regarding IP addresses.

3 Enterprise Console and Web Appliance

When a Full Web Control policy is applied using either a Sophos Web Appliance or Sophos Management Appliance, Enterprise Console supplies the hostname of the corresponding appliance so that endpoints can communicate with it, either directly or through Sophos LiveConnect.

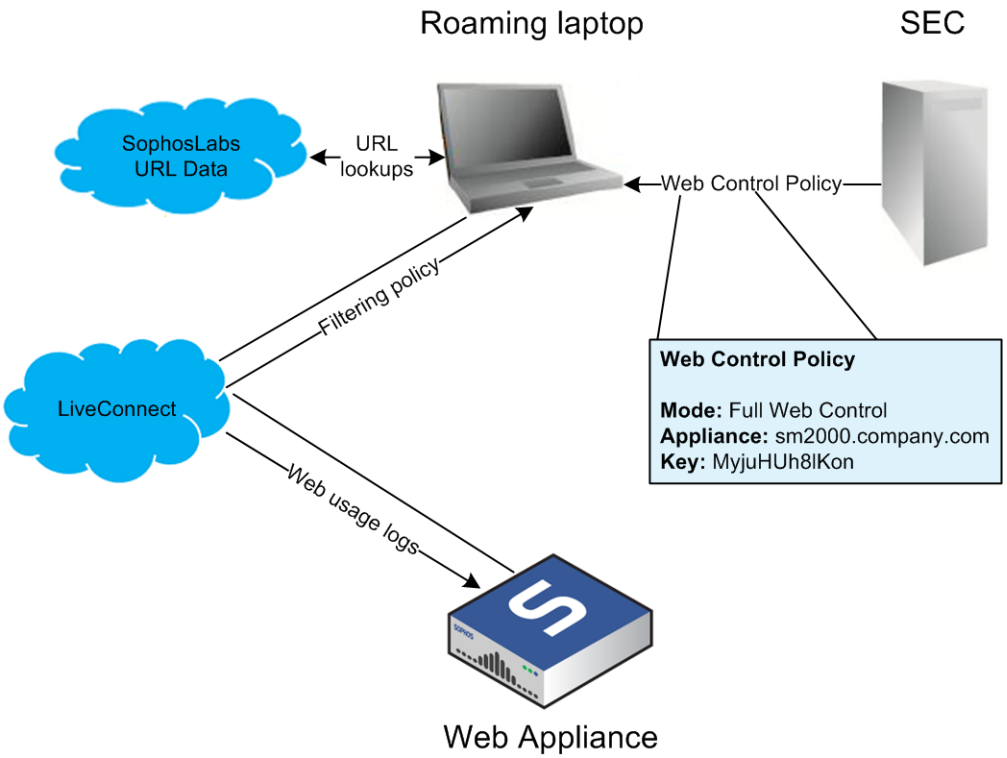
Sophos LiveConnect is a central cloud-based service that allows you to always manage all of your endpoints, whether they are on your local network, at remote sites, or with traveling users.

3.1 Enterprise Console and Web Appliance without LiveConnect



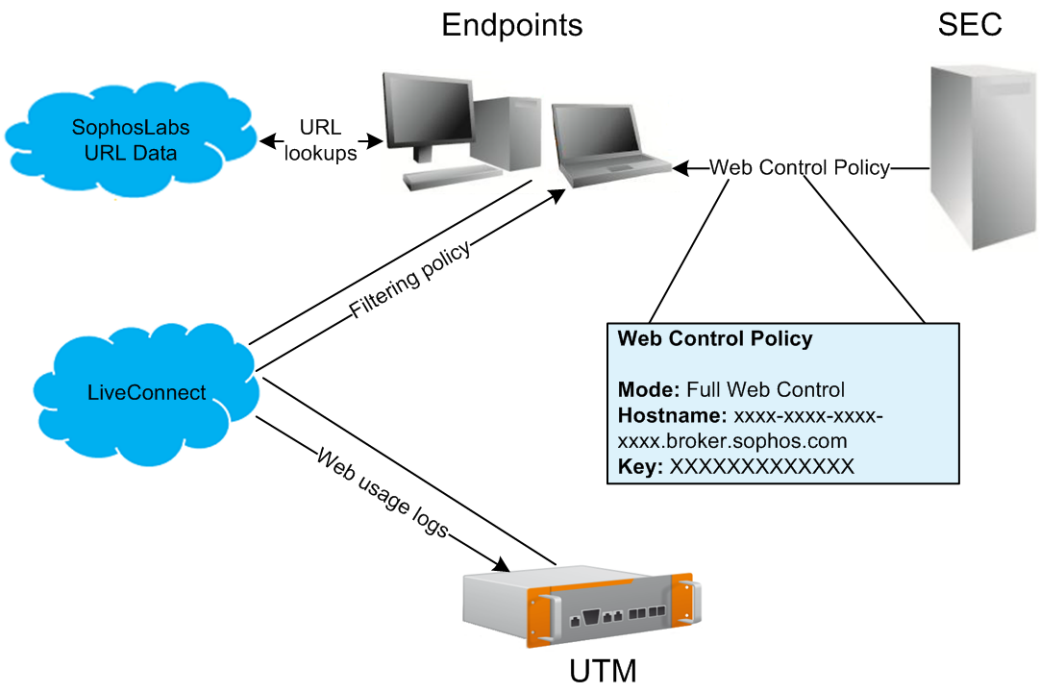
When a Full Web Control policy is applied using either a Sophos Web Appliance or Sophos Management Appliance without Sophos LiveConnect enabled, the users’ endpoint software connects to that appliance and obtains a complete web-filtering policy. Users’ web activity data is sent back to the designated appliance, while web event data (websites scanned and assessed by the live URL-filtering feature) is sent to Enterprise Console.

3.2 Enterprise Console and Web Appliance with LiveConnect



Optionally, you can deploy Full Web Control with Sophos LiveConnect enabled on the Web Appliance. With LiveConnect, users have access to a cloud service that allows roaming endpoints to communicate with the appliance without you having to allow special access through your organization's firewall.

4 Enterprise Console and UTM



UTM uses Sophos LiveConnect—a central cloud-based service—for protecting and monitoring endpoint computers. Policy updates are distributed to users, and reporting data from endpoint computers is uploaded, even when users are not connected from within the network.

When a Full Web Control policy is applied using a Sophos UTM appliance, Enterprise Console supplies the hostname of the Sophos LiveConnect broker used by UTM so that endpoints can communicate with it. The users' endpoint software connects to that host and obtains a complete web-filtering policy. Users' web activity data is sent back to the appliance via LiveConnect, while web event data (websites scanned and assessed by the live URL-filtering feature) is sent to Enterprise Console.

5 Benefits of endpoint web control

While the Sophos Web or UTM appliance provides security and productivity protection for systems browsing the web from within your corporate network, endpoint web control extends this protection to users' machines. This provides protection, control, and reporting for endpoint machines that are located, or roam, outside your corporate network.

Enterprise Console can deliver web control policies to your endpoint machines that provide malware protection and productivity rules based on common site categorizations. With the combination of Sophos Enterprise Console and a Sophos Web or UTM appliance it is possible

to extend your full web policy to endpoint machines, providing more than 50 site categories, highly flexible policy configuration, and detailed reporting on threats and usage.

With Sophos LiveConnect, roaming machines will still receive full web policy updates, and will provide web usage logs back to the appliance, from wherever it connects, without having to use a VPN or configure special network settings.

6 Legal notices