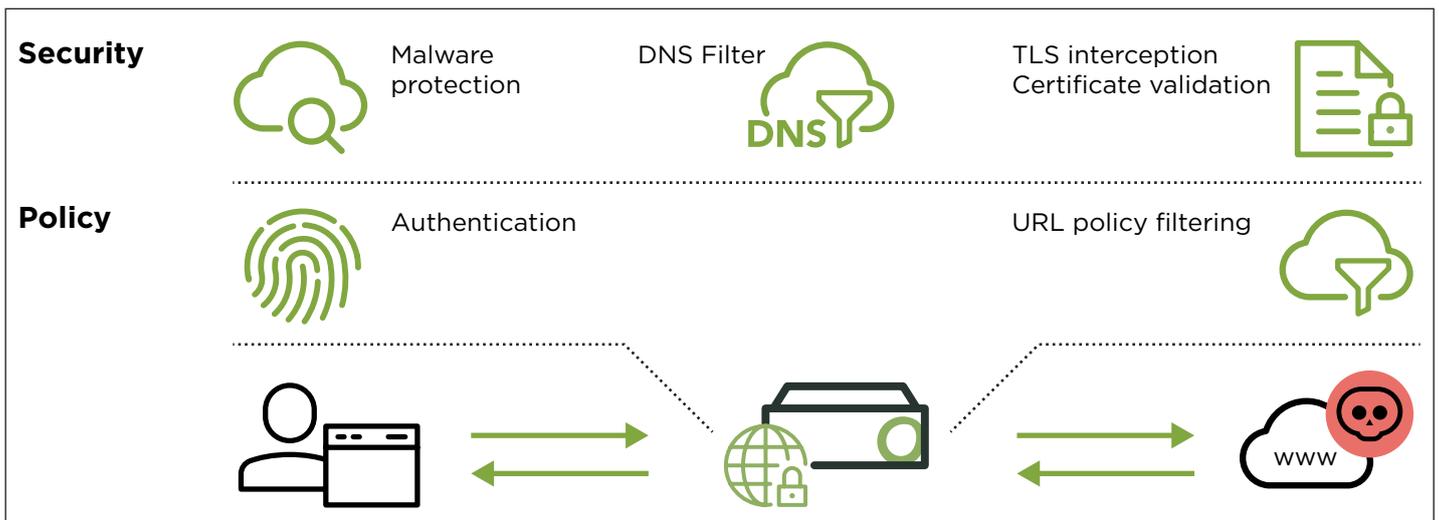# Secure Web Gateway

open systems

PRODUCT BRIEF

Control and protect your users' web traffic

Why do we need to filter web traffic?

Every organization should have a global internet access security policy – not only to protect day-to-day operations but to defend its brand. Open Systems' Secure Web Gateway ensures that the network-wide web usage is business aligned and that users are shielded from malicious web content.

How we protect your network

From a policy perspective, the Secure Web Gateway enables organizations to easily manage the enforcement of company business policies through customizable user groups (authentication) and category-based URL and DNS filtering. At the same time, since most successful cyberattacks start with browsing a compromised website, the Secure Web Gateway provides various threat protection measures – such as URL and DNS filtering, malware protection, TLS interception or certificate validation – to help prevent security breaches.

Security	Malware protection	DNS Filter	TLS interception Certificate validation
Policy	Authentication		URL policy filtering

The Secure Web Gateway helps protect from web threats and enforce your business policy

Authentication

Create policy groups and different levels of malware protection, URL filtering or TLS interception for different departments or groups of people.

Seamless authentication can be enabled using Kerberos tickets issued by your existing Active Directory infrastructure.

Malware protection

Protocol scanning technologies for HTTP and FTP traffic are used and combined with filters to detect both known and unknown malware.

With TLS interception also encrypted traffic can be scanned for any malicious content.

Expert-level operations

Enjoy the peace of mind that 24x7 monitoring, incident handling, and change management brings – provided by our L3 engineers.

Central policy setup and control allows you to enforce global security policies and configuration.

Secure Web Gateway highlights

Authentication of users enables the creation of different policy groups and different levels of malware protection, URL filtering, and SSL scanning.

URL Filter enforces an organization's internet access policy and protects against risks associated with employees' internet use.

TLS interception and Certificate Validation applies an existing security and internet usage policy to the HTTPS protocol, expanding coverage of an organization's policy to encrypted traffic (about 85% of all web traffic these days) and preventing viruses, spyware, and Trojans from bypassing malware protection by using HTTPS encryption.

Malware Protection uses protocol scanning technologies for HTTP and FTP, as well as a combination of filters, to detect both unknown and known malware. One highlight is the ability to filter for malicious macros of all Microsoft Office files (Excel, Word, etc.).

Authentication

URL Filter

TLS Interception & Certificate Validation

Malware Protection
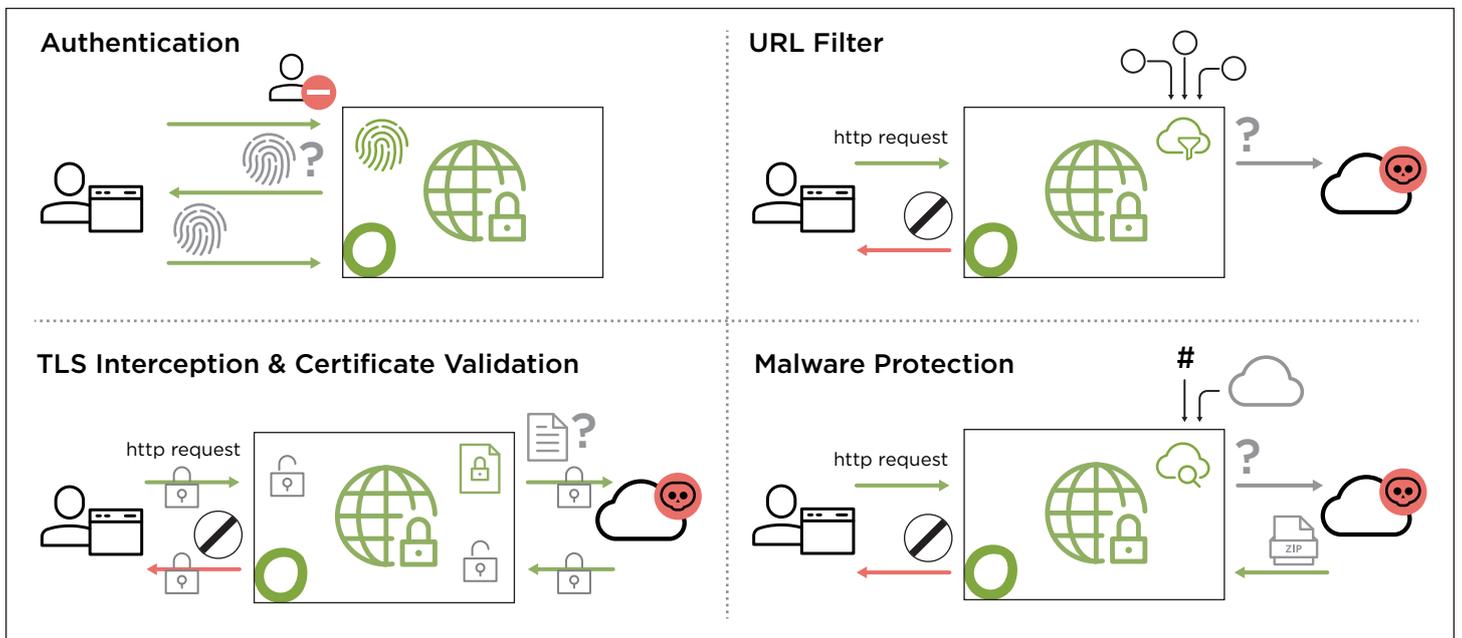
Global overview and configuration

The Customer Portal provides an overview of all your users' web traffic no matter where they are located. In addition, drill-down options provide a high granularity level such as domains, countries, applications or endpoints.

Secure Web Gateway configuration is always global which is especially useful for traveling users as the experience stays the same irrespective of the users' locations. Applications are matched with the same engine used already in other features of the Secure SD-WAN stack.

Co-management

If desired, leverage the Secure Web Gateway self-service features in the Open Systems Customer Portal that allow you to apply changes yourself. Mission Control will, of course, still be there to support you if you have questions.

The intuitive self-service tool will lead you through the change steps and provide you with useful information at every stage. Observe the deployment of your change in real time through the job schedule overview.

open systems