Forcepoint

Solution Brief

Zero Trust Content Disarm and Reconstruction for Gateways

Web Download

Challenge

› To ensure that files downloaded from the internet do not contain malware without security measures interfering with user experiences.

Solution

› A GX Appliance connected to an ICAP-enabled web gateway protects users from unsafe files downloaded from the Internet.

Outcome

› Users can download content such as images, documents and PDFs safely with the knowledge that they have been rendered and malware free.

File Download

Challenge

› To ensure that files uploaded by external sources, customers or partners to web portals do not contain malware.

Solution

› A GX Appliance connected to an ICAPenabled web application firewall protects organisations from unsafe files uploaded from the Internet.

Outcome

› Organizations can open and use uploaded files safely with the knowledge that threats have been removed.

Forcepoint's Gateway eXtension (GX) Appliance provides Zero Trust Content Disarm and Reconstruction (CDR) as an extension to web security gateways that support Internet Content Adaptation Protocol (ICAP). Zero Trust CDR ensures content passed to it from the gateway is made safe by removing the threat of malware. This paper will outline the requirements that a gateway will need to fulfil to be able to use a GX appliance via the ICAP protocol, with alternatives if ICAP is unable to be used.

ICAP Protocol

ICAP was designed to extend the capability of proxy servers to free up their resources. The protocol allows for proxy servers to offload processing of data to external servers to perform tasks such as antivirus scanning and content filtering, leaving the proxy servers to focus on scaling to meet throughput requirements. Proxy servers can use the results from the external processing to either decide to allow/block the content or to modify it.

Request Modifications

When a request is made for a web page, it can be passed via ICAP to an external server to handle it. This may be to perform a check on the URL that is being requested or it may be to ensure content that is being uploaded is allowed to be sent. This is known as **reqmod** in the ICAP protocol. The external server can either modify the content (e.g. make it safe to upload) or provide a yes / no answer indicating to the proxy whether the request should be allowed.

Response Modifications

When data is returned from the web page, it can be passed via ICAP to an external server to handle it. This is usually to ensure that the content being downloaded is safe to receive. This is known as **respmod** in the ICAP protocol. The external server can either modify the content (e.g., make it safe to download) or provide a yes/no answer indicating to the proxy whether the response should be allowed.

Forcepoint's GX Appliance

Zero Trust CDR is a highly effective approach for removing malware from data. Unlike traditional forms of stopping malware such as antivirus and sandboxing, it does not rely on detection and so new, unknown malware is stopped just as easily as existing, known malware. **The GX Appliance is an implementation of Zero Trust CDR that can be plugged into gateways to enhance their malware prevention capabilities.** To ascertain whether a gateway will work with the GX Appliance, the following need to be considered:

ICAP Channels

Gateways may already be using ICAP for processing content (e.g. for DLP). The gateway must be able to support one or more additional ICAP channels for connections to the GX Appliance.

Safe Download

To support safe download of files and other static content from the Internet (e.g., images), the gateway must support:

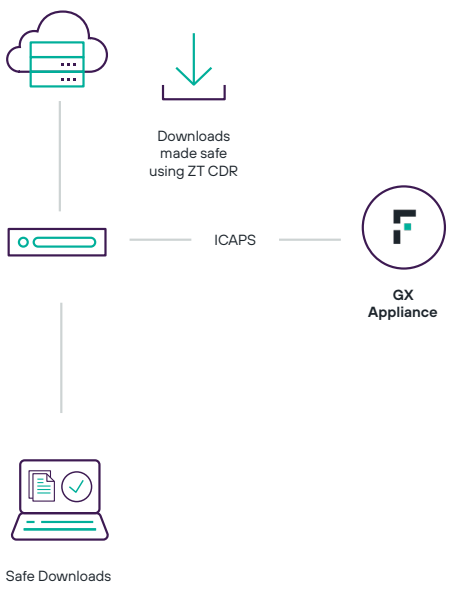
- → Configuration of ICAP **respmod** settings to be able to send responses to GX Appliance.
- → Sending on the modified content returned from the GX appliance on to the browser.

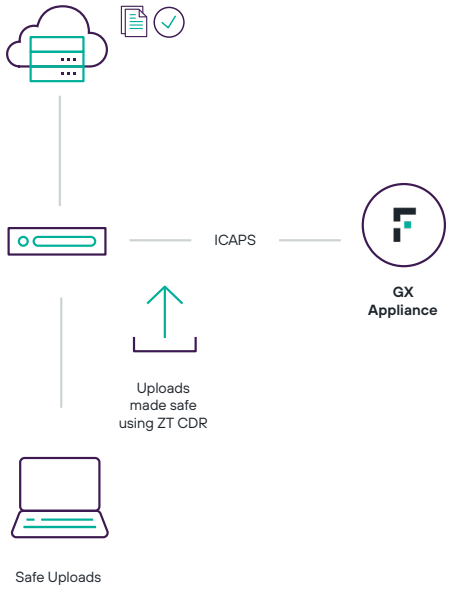
Safe Upload

To support safe upload of files to the internet, the web gateway must support:

- → Configuration of ICAP **reqmod** settings to be able to send requests to the GX Appliance;
- → Sending on the modified content returned from the GX Appliance on to the web server.

In addition to this, some web applications such as Twitter, Facebook etc. use a proprietary API when uploading files. This allows files to be uploaded in chunks to the application. To support safe upload to these applications, the gateway has to support the application-specific API in order to collate and pass the GX Appliance the entirety of the data being uploaded so that it can be made safe.





Selected File Types

The GX Appliance will apply Zero Trust CDR to file formats that it can natively handle. All other file types will be returned unchanged. A gateway that supports sending selected file types to the GX Appliance will be more efficient since it will only pass data to the GX that can be handled, thus not wasting bandwidth.

TLS

The ICAP connection between the gateway and GX Appliance can be secured using TLS (ICAPS). The GX Appliance supports ICAPS and this is the recommended way of connecting into a gateway. The GX can be configured with either server or mutual authentication. In these cases, a private key and certificate are required to be uploaded to the GX Appliance.

Profile Switching

The GX Appliance supports multiple configurations (profiles) allowing different policies to be applied for different traffic. e.g., whether or not to retain macros in Office documents. To support this, the GX Appliance chooses the profile to apply based on the value of a configured ICAP protocol header.
A gateway can use this feature by passing different values for the configured ICAP header for different traffic types. This could be used, for example, to have different configuration for different users or groups of users.

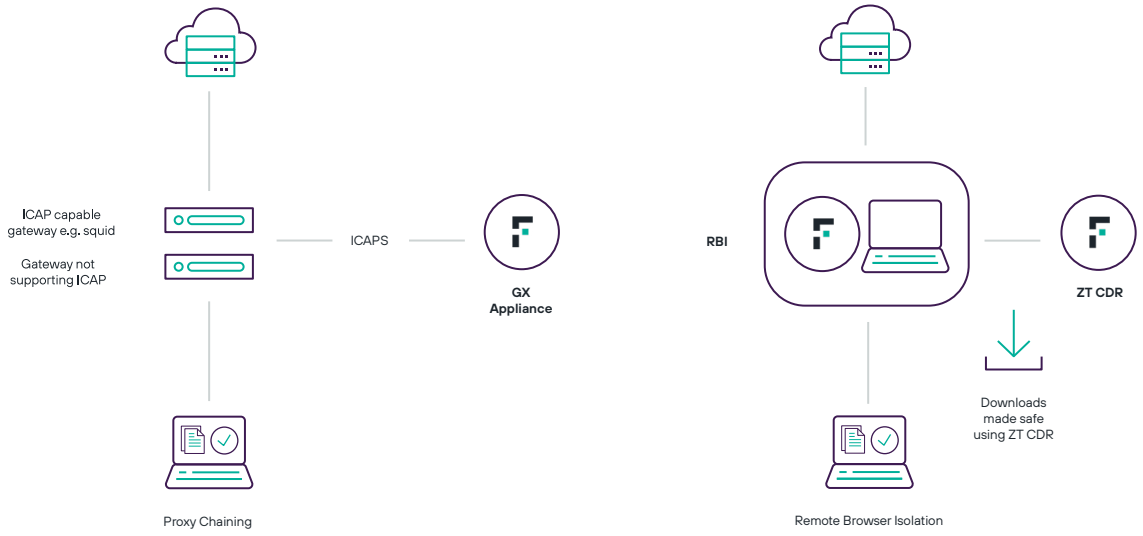
Availability / Resilience

A farm of GX Appliances can be used to provide resilience and availability. To support this, the gateway must support the configuration of a list of addresses to try or an external load balancer is required. To prevent each GX Appliance from being overloaded, the gateway should support the "max connections" limit.

Zero Trust CDR when a Gateway does not fully support ICAP

Some gateway products do not fully support ICAP (either by not handling modified content in the response or not supporting configuration of the relevant ICAP command (reqmod, respmod). In this case, Zero Trust CDR can still be added to an architecture in two different ways

- → Proxy chaining to a second gateway that does support the necessary features of ICAP. Squid is a popular open-source gateway that supports all the necessary ICAP features to work with GX Appliance and can be used in a proxy chain.
- → Forcepoint Remote Browser Isolation (RBI) provides a safe isolated environment in which to browse web sites and when files need to be downloaded to the desktop out of the isolated environment, Forcepoint RBI sends the files to an inbuilt Zero Trust CDR service to make them safe first.



Summary

The GX Appliance can be deployed with a gateway to provide Zero Trust CDR. To use GX, the gateway must support passing on the modified data returned from the GX. To support safe download of content, the gateway must support the respmod configuration. If looking to protect file uploads it must support the reqmod configuration and, in this case, there is the additional consideration as to whether web applications are being used that use a proprietary API.

There are additional features of the GX that can be used where the gateway has the capabilities to select the file types sent, use ICAPS and be able to pass custom ICAP headers.

Where an existing gateway does not support the necessary ICAP features, proxy chaining or Remote Browser Isolation (RBI) can be used to add Zero Trust CDR protection.

Zero Trust CDR direct Integrations

- → McAfee Web Gateway (on-premise / cloud)
- → McAfee Unified Cloud Edge (SaaS)
- → iboss Secure Cloud Gateway (SaaS)
- → Squid
- → Broadcom Symantec ProxySG*
- → Fortinet Fortigate Firewall

* ProxySG supports only one ICAP device per direction (request / response)

Zero Trust CDR by Proxy Chaining or RBI

- → Forcepoint Secure Web Gateway
- → Forcepoint NGFW
- → ZScaler
- → Palo Alto NGFW
- → Trend Micro
- → Cisco Web Security Appliance

forcepoint.com/contact