censornet.

Web Security Best Practices

Contents

censornet.

Web Security Best Practice

This guide outlines Censornet's best practice for Web Security

NOTE: This is a recommendation based on our experience.

Block Unclassified Site

Feature: Block Unclassified Sites by default – By enabling this feature, our solution will **block** access to sites that the categorisation engine has not classified yet. This could be because the site is very new or no requests have been made to that site etc.

KB link - https://help.clouduss.com/ws-knowledge-base/unclassified-uncategorised-site-processing

Why do we recommend: To prevent access to sites that are yet to be classified and therefore potentially malicious

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/product-web-security/templates

Tips: If you believe a URL to be incorrectly classified, you can submit a classification request via the dashboard.

KB link - https://help.clouduss.com/ws-knowledge-base/how-to-submit-a-url-reclassification-request

If you require immediate access to the site, you can achieve this via the use of Custom URLs.

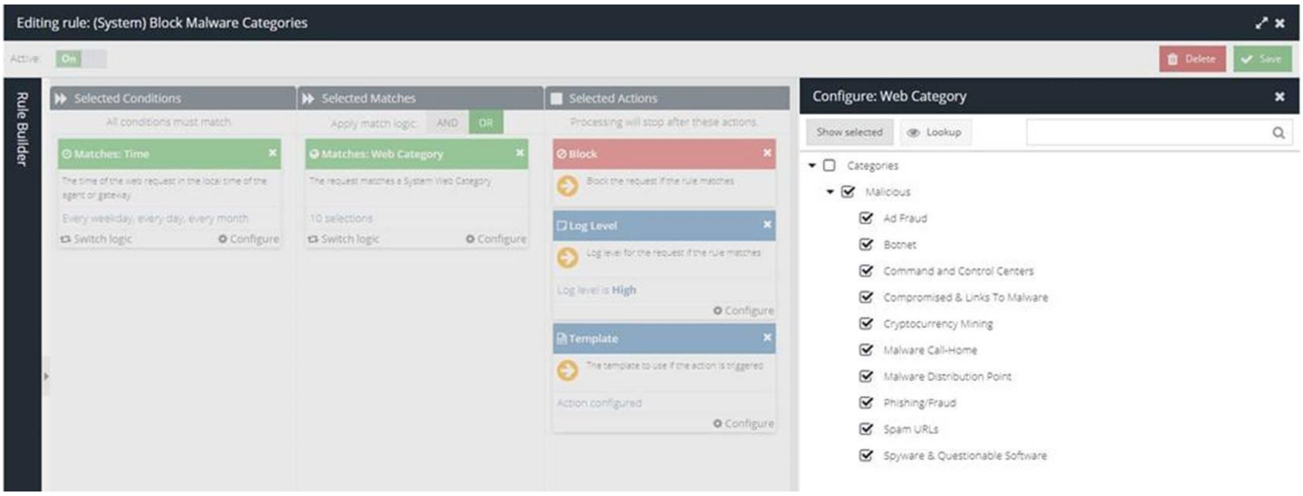
KB link - https://help.clouduss.com/product-web-security/custom-urls).

Rule Prioritisation

Feature: Rule Prioritisation – By ensuring the correct ordering of rules, you can maintain security. Rules are processed from top to bottom with rules only being triggered if the "conditions" and "matches" within the rule are met. Once a rule is triggered, no further rules are evaluated. If no explicit rules are triggered a built in hidden rule ensures the default action on the web request will be allowed (This behaviour can be reversed through the use of an explicit catch-all block rule)

Why do we recommend: It is always recommended to have the (System) Block Malware Categories rule as the first rule within the Filter Rules list to ensure that URLs within these categories are always blocked. This helps to avoid situations, where URLs that were once safe and have been dynamically reclassified due to malicious content being found, are still blocked.

How to configure: Please see the screenshot below to configure the recommended "Block Malware Categories" Rule under **products>Web Security>Filter Rules**



Editing rule: (System) Block Malware Categories

Active: On

Selected Conditions

All conditions must match

Matches: Time

The time of the web request in the local time of the agent or gateway

Every weekday, every day, every month

Selected Matches

Apply match logic: AND [✓ OR]

Matches: Web Category

The request matches a System Web Category

10 selections

Selected Actions

Processing will stop after these actions

Block

Block the request if the rule matches

Log Level

Log level for the request if the rule matches

Log level is **High**

Template

The template to use if the action is triggered

Action configured

Configure: Web Category

- □ Categories
  - ☑ Malicious
    - ☑ Ad Fraud
    - ☑ Botnet
    - ☑ Command and Control Centers
    - ☑ Compromised & Links To Malware
    - ☑ Cryptocurrency Mining
    - ☑ Malware Call-Home
    - ☑ Malware Distribution Point
    - ☑ Phishing/Fraud
    - ☑ Spam URLs
    - ☑ Spyware & Questionable Software

Tips: To gain further understanding of rule logic, please see the kb article.

KB link - https://help.clouduss.com/product-web-security/standard-rules

Mime Type Filtering

Feature: Mime Type Filtering – Restrict Mime Types that can be downloaded from the Web

Why do we recommend: The download of certain Mime Types increases the potential security risk to an organisation (e.g. executables). Use this feature to ensure a user can only download Mime types that are approved by the organisation.

How to configure: Restrict what users are allowed to download by ensuring that relevant Filter Rules with the action of Allow also have a response action of MIME Type. When a MIME type category is selected from the list, it ensures that the downloading of the selected MIME-type is no longer permitted.

KB link - https://help.clouduss.com/product-web-security/rules-engine-concepts#mime_type

Tips: Ensure you are aware of the implications of blocking certain file types (e.g. Javascript)

Malware Scanning (License Required)

Feature: Malware Scanning of content.

Why do we recommend: By enabling the malware scanning capability within the agent(s), you will improve your environment's security posture by having the ability to scan requested content and blocking access if the contact is deemed malicious.

How to configure: Follow this KB article on how to configure this feature (only available if the Malware Scanning license has been purchased and applied).

KB link Windows - https://help.clouduss.com/agents/configuration-options-for-the-windows-agent-type#agent_anti_malware

KB link Gateway - https://help.clouduss.com/agents/configuration-options-for-the-gateway-agent-type#gateway_anti_malware

KB link Mac OSX – https://help.clouduss.com/agents/configuration-options-for-the-mac-os-x-agent-type#agent_anti_malware

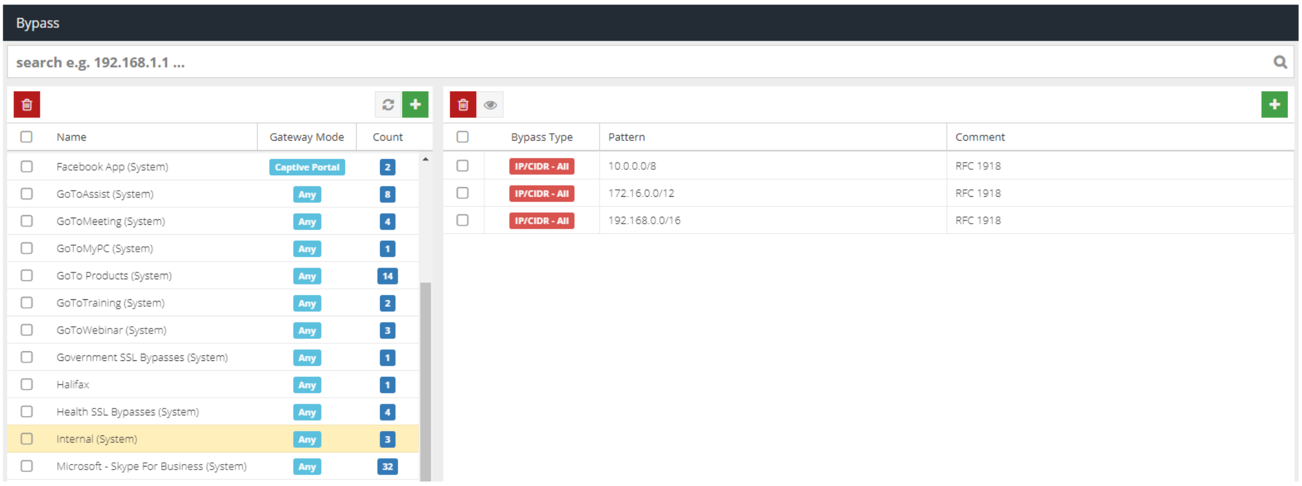
Tips: You can adjust the size of files that are scanned if required.

Internal Bypass

Feature: Have a Bypass list of internal address.

Why do we recommend: Our solution only knows about public sites and application, if you host your own site and application on your internal network then access may be blocked unless you configure a bypass group for the internal address.

How to configure: Please see the screenshot below to configure the recommended "Internal (System)" Bypass under **products>Web Security>Bypass**



Bypass

search e.g. 192.168.1.1 ...

□	Name	Gateway Mode	Count
□	Facebook App (System)	Captive Portal	2
□	GoToAssist (System)	Any	8
□	GoToMeeting (System)	Any	4
□	GoToMyPC (System)	Any	1
□	GoTo Products (System)	Any	14
□	GoToTraining (System)	Any	2
□	GoToWebinar (System)	Any	3
□	Government SSL Bypasses (System)	Any	1
□	Halifax	Any	1
□	Health SSL Bypasses (System)	Any	4
□	Internal (System)	Any	3
□	Microsoft - Skype For Business (System)	Any	32

□	Bypass Type	Pattern	Comment
□	IP/CIDR - All	10.0.0.0/8	RFC 1918
□	IP/CIDR - All	172.16.0.0/12	RFC 1918
□	IP/CIDR - All	192.168.0.0/16	RFC 1918

KB link - https://help.clouduss.com/product-web-security/bypass-categories

Tips: Once you have configured a Bypass Category ensure you assign it to the required agent profile.

Browser Categories

Feature: Browser Categories Rule Condition

Why do we recommend: Browser Categories allow admins to create a collection of browsers and version number patterns, which can be used as part of the Browser Type condition in Filter Rules. Browser Categories allow you to control the types of browsers and version used within your organisation. Typically, this can be used to block vulnerable browsers or unsanctioned browser versions from connecting to the Internet.

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/product-web-security/browser-categories

Tips: Ensure your rule that blocks browser types or version is placed at the top of the rule base.

Operation System

Feature: Operation System Rule Condition

Why do we recommend: An Operating System Rule Condition allows admins to create Filter Rules to control the types of Operating System and version used within your organisation. Typically, this can be used to block vulnerable Operating Systems or unsanctioned Operation System versions from connecting to the Internet.

How to configure: Follow this KB article on understanding Filter rule logic and apply the Operation System option as a condition.

KB link - https://help.clouduss.com/product-web-security/standard-rules

Tips: Ensure your rule that blocks Operation System or Operation System version is placed at the top of the rule base.

MFA on Admin account.

Feature: Enabling MFA on any admin account.

Why do we recommend: By enabling MFA on admin accounts, the authentication process will be improved by adding an extra layer of security via a simple SMS based OTP (One Time Passcode).

How to configure: Follow this KB article on how to configure this feature.

KB link – https://clouduss.helpdocs.io/settings/account-password-and-mfa

Tips: You can suspend users accounts if they have not enabled MFA on their account.

KB link Learn about types of admin roles - https://help.clouduss.com/settings/roles

Admin Audit License

Feature: Admin Audit license

Why do we recommend: By enabling the admin audit feature, administrators have a high-level history of activity carried out by administrator users within the **USS** dashboard.

How to configure: To check if you have the license, please view the kb article.

KB link – https://help.clouduss.com/account-settings/licenses

Cloud Gateway TLS/SSL Inspection

Feature: TLS/SSL Inspection.

Why do we recommend: By enabling TLS/SSL inspection on a Cloud Gateway HTTPS as well as HTTP traffic can be inspected. This ensures modules such as Malware Scanning, Image Scanning and CASB have visibility and policy can be enforced.

How to configure: Follow this KB article on how to configure this feature.

KB link – https://help.clouduss.com/agents/configuration-options-for-the-gateway-agent-type#tls_ssl_interception

Tips: Please see other options available on the cloud gateway.

KB link Learn how to enable image analysis (License required) - https://help.clouduss.com/agents/configuration-options-for-the-gateway-agent-type#image_analysis

KB link Captive/Guest Portal - https://help.clouduss.com/agents/configuration-options-for-the-gateway-agent-type#captive_guest_portal

Active Directory

Feature: Active Directory Integration

Why do we recommend: By enabling Active Directory integration, you can create user-based filtering rules, either by AD User, AD Security Group or AD OU which can make creating filter rule logic a straightforward task.

How to configure: Follow this KB article on how to configure this feature.

KB link – https://help.clouduss.com/settings/active-directory

Tips: Get the most out of Active Directory integration by understanding our filter rules.

KB link - https://help.clouduss.com/product-web-security/standard-rules#selected_conditions