# Secure Internet Access

Mani Shankar Kumar

*Sr. System Engineer, Gilead Sciences Inc.*

## I. WHAT IS SECURE INTERNET ACCESS.

Citrix Secure Internet Access (CSIA) is a cloud-based solution that enables secure remote access to online and SaaS applications. It includes a secure web gateway, a cloud access security broker, malware protection with sandboxing, intrusion detection and prevention systems, and data loss prevention. Along with SDWAN and Secure Workspace Access, Citrix Secure Internet Access is a cornerstone of Citrix's fully integrated Secure Access Service Edge (SASE) solution.

Citrix Safe Internet Access allows safe access to online and SaaS applications both within and outside the Citrix Workspace, regardless of the user's location. It adds an additional layer of protection to Citrix Workspace users and integrates with Citrix SDWAN to provide a fully integrated Citrix network and security solution.

## II. FEATURES AND BENEFITS OF CITRIX SECURE INTERNET ACCESS

Citrix Secure Internet Access facilitates in the centralized management of Citrix Cloud-based services. The capabilities and benefits of Citrix Secure Internet Access are summarized as below,

A. Unified management:

- Comprehensive security capabilities with a holistic view and granular control. This is all available on a single platform, together with analytics for detecting security incidents, out of the ordinary behavior, reported risks, productivity loss, and policy breaches.
- Users that have access to both SDWAN and Citrix Secure Internet Access can manage both services from the same interface. As a result, all traffic and users are safeguarded using a platform that combines network and security designs.

B. Efficiency:

- Citrix SDWAN and Citrix Secure Internet Access implementation is simple and quick, with automatic configuration.
- High-performance design with cloud-like scalability.
- For best speed, a single pass architecture is used, in which communication is decrypted once and all security measures are executed before being re-encrypted.
- SDWAN reduces latency by automatically selecting the closest Citrix Secure Internet Access gateway node.

C. Reliable performance

- Updates are delivered automatically to ensure that you have the most up-to-date protection against security risks.
- Backup connections for dual resiliency.
- Because of the single, unified view, IT can troubleshoot issues more quickly.

D. Privacy

- In the Citrix Secure Internet Access service, each customer's data is processed through distinct gateways and separated by enterprise. Data is reviewed and logged locally to ensure GDPR compliance.

E. Better remote working user experience

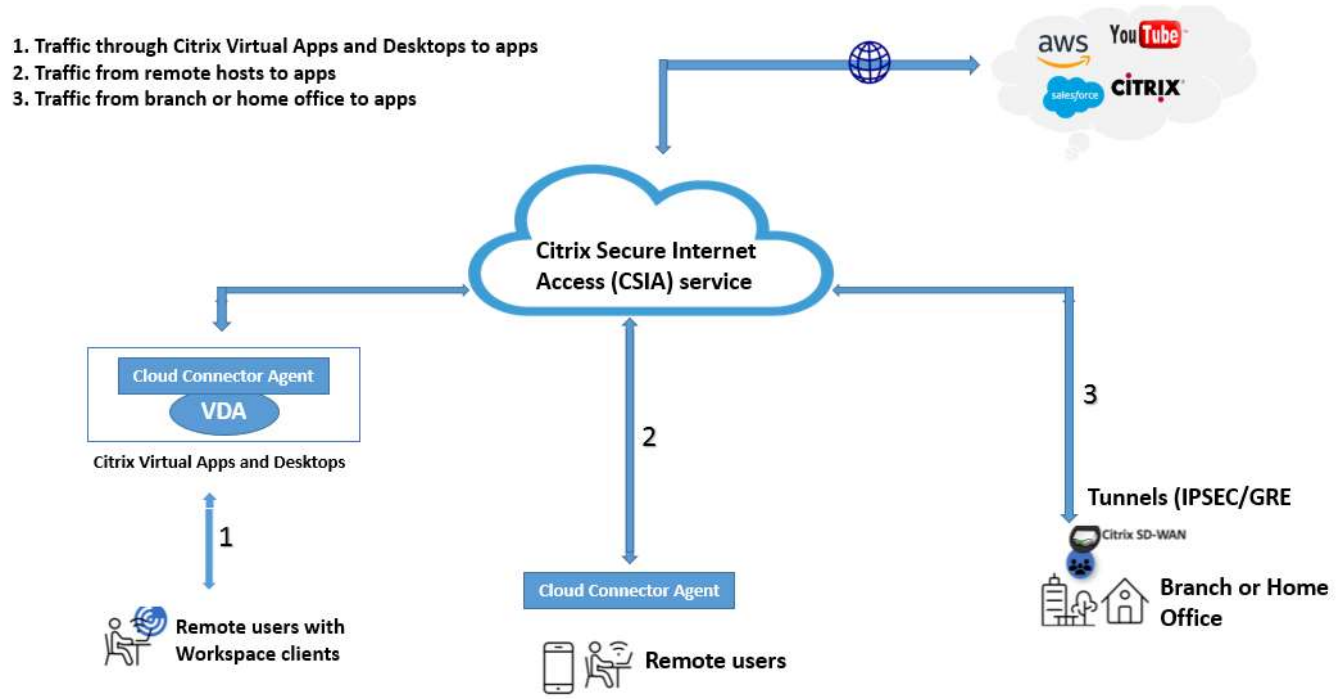
- Moving network security to the cloud, where the resources that users need are already available, brings security closer to the users. Citrix Secure Internet Access has over 100 points of presence (PoP) around the world.

## III. HOW CITRIX SECURE INTERNET ACCESS WORKS

One of the following ways may be used by your users to access unapproved web and SaaS applications:

• utilizing Citrix Workspace to create virtual desktops
• from a branch or home office
• remotely from local host systems

Regardless of the user's mode of direct internet connection, traffic is diverted through Citrix Secure Internet Access.




The three key use cases represented in the preceding image describe how the process works.

1. **Citrix Virtual Apps and Desktops**: - Remote users may safely access unauthorized web and SaaS applications with Citrix Virtual Apps and Desktops. Install a CSIA Cloud Connector agent on the Virtual Delivery Agent to reroute internet traffic (VDA).
2. **Native browsers on host systems:-** Remote users may safely access unapproved software on their local systems (laptops, phones) (managed or unmanaged). Install CSIA Cloud Connector agents to encrypt internet traffic on these devices. The Cloud Connector agent authenticates users and installs SSL certificates. The Cloud Connector has agents for iOS, macOS, Android, Windows, and Linux.
3. **Branch offices**: - On-premises users may securely access online and SaaS programs by routing traffic to Citrix Secure Internet Access. IPSEC or GRE tunnels are used to do this without a Cloud Connector agent. Assembles secure connection to the closest Citrix Secure Internet Access point of presence (PoP). Traffic is tunneled using IPsec or GRE. Multiple connections to main and secondary Citrix Secure Internet Access PoPs provide redundancy.
4. **Licensing: -** Citrix Secure Internet Access (CSIA) is available in three editions.

**Standard**: A cloud-based security system with centralized management. CASB, SSL traffic management, and web content screening are important security elements.

**Advanced**: Complete security solution includes malware detection, command and control callback detection, and incident response.

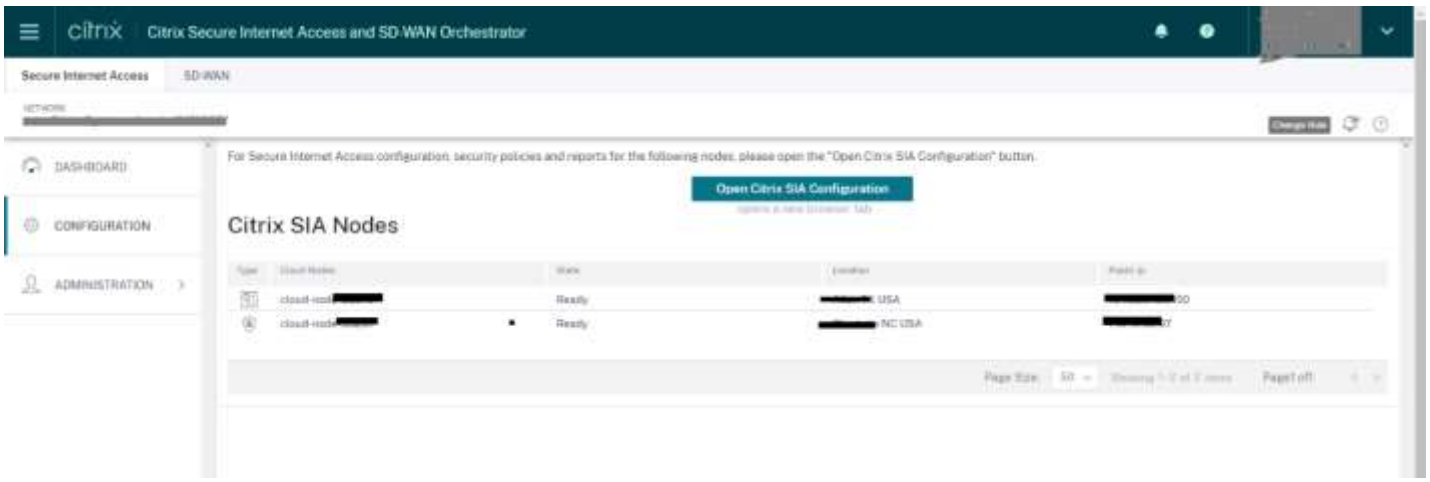
**Premium**: This complete security solution includes superior sensitive content detection and analysis.

I've set up a laboratory environment to demonstrate how to configures citrix secure internet access.

**Step-1: Log into Secure Internet Access**

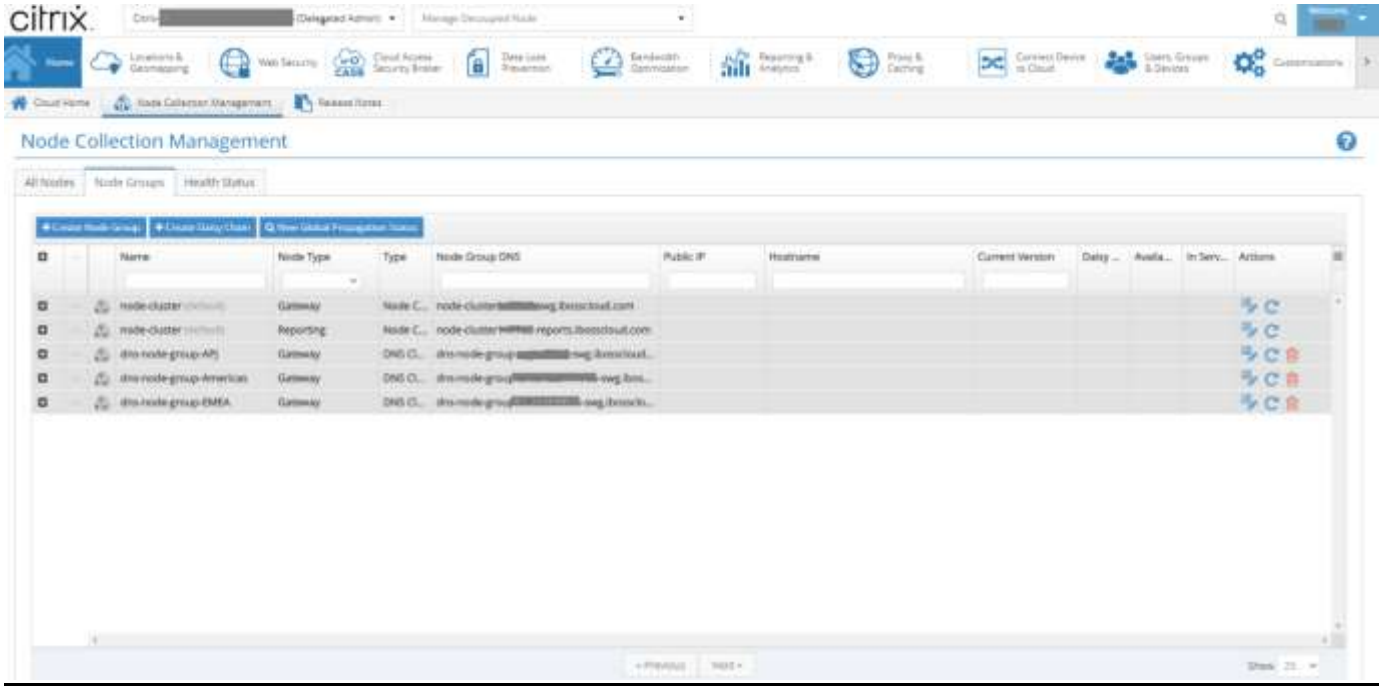
Log into Citrix Cloud (https://citrix.cloud.com) and click on **CSIA Admin UX** account within the customer list

- Ensure the **OrgID** in the top right matches the Network **OrgID** on the left side. If that is different, select **Change Role.**
- Select the **Configuration** tab
- Select the **Open Citrix SIA Configuration** button




**Step-2: Home -> Node Collection Management -> Node Groups**

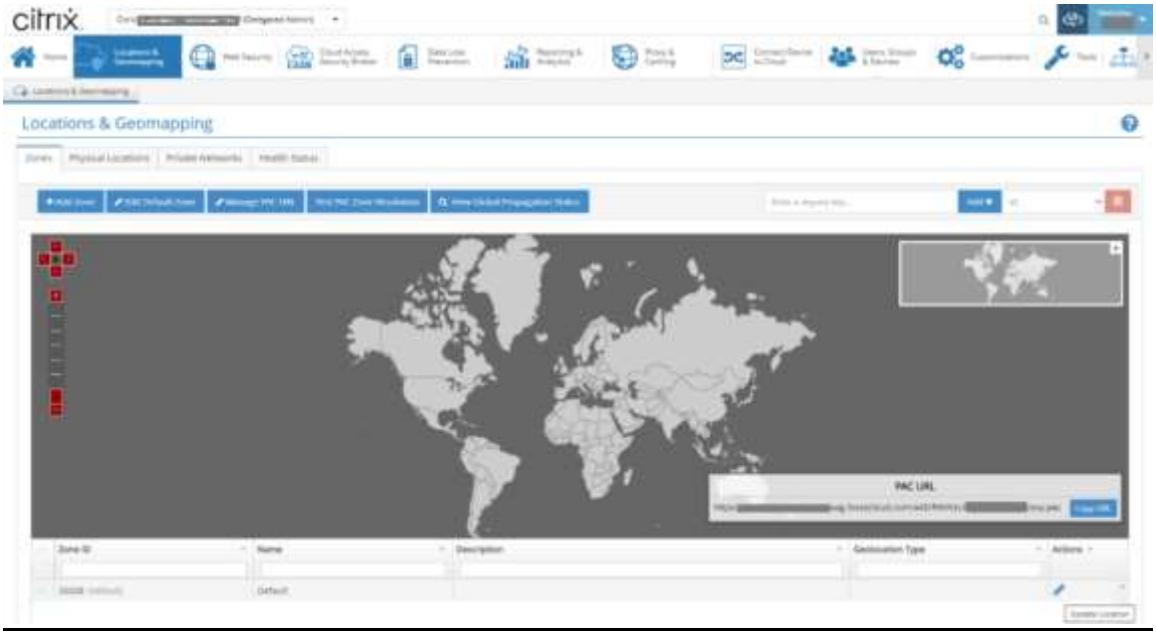
- Make sure you have at least one Gateway Node Cluster




- Document this **hostname** and **IP Address** for later validation as it should appear in your PAC file

**Step-3: Configuring PAC Settings**

- Click on **Edit Default Zone**

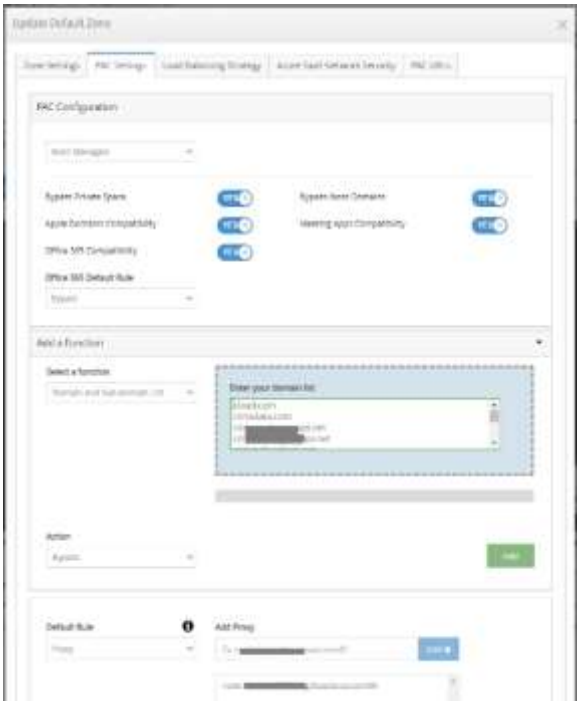



**Step-5: Update Default Zone Dialog -> PAC Settings**

Use the "**Add a Function**" to add a "**Domain and Sub-domain List**" function containing Citrix Cloud domains,

- cloud.com
- citrixdata.com
- citrixworkspaceapi.net
- citrixnetworkapi.net
- xendesktop.net

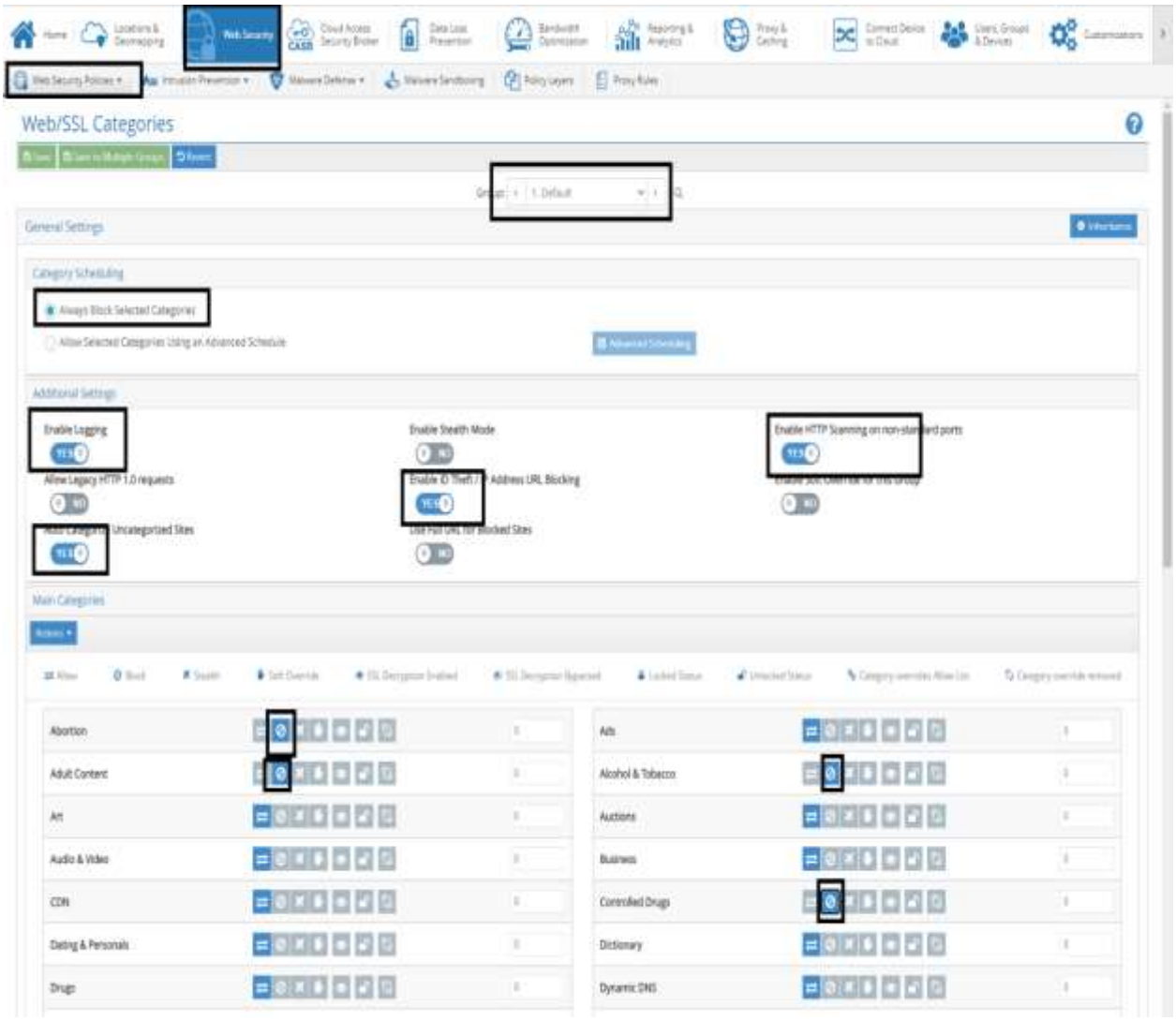
Any traffic destined for these URLs will not traverse the SIA service



**Step-6: Web Security**

- This is the main place where we set actions on web categories.
- Notice the Group Selector at the top, if you wanted to apply different settings to different groups.

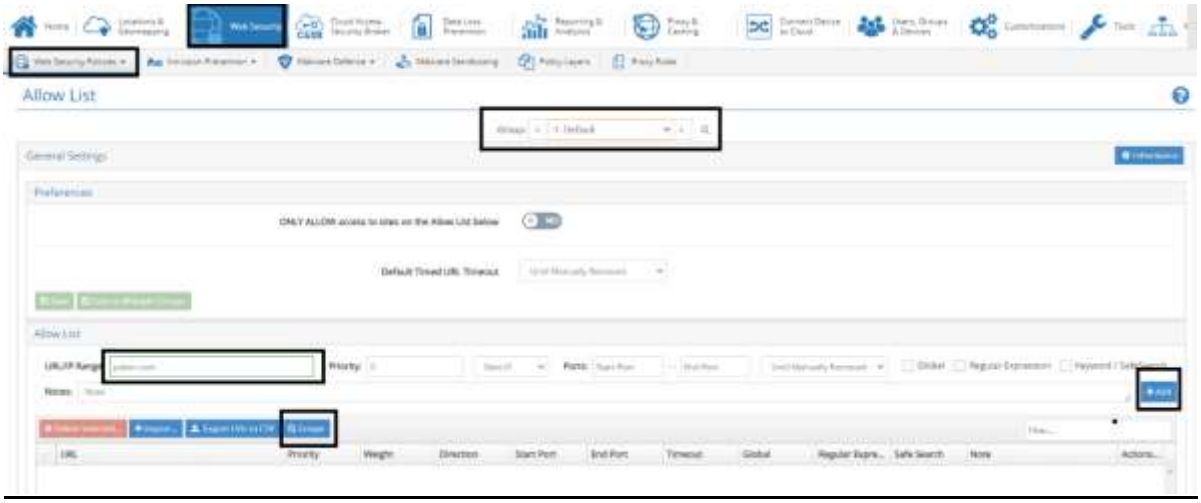

- (Optional) Turn on **Enable ID Theft / IP Address URL Blocking**. This will block IP addresses to be used to access a website.




- Turn on **Enable HTTP Scanning on non-standard ports.**

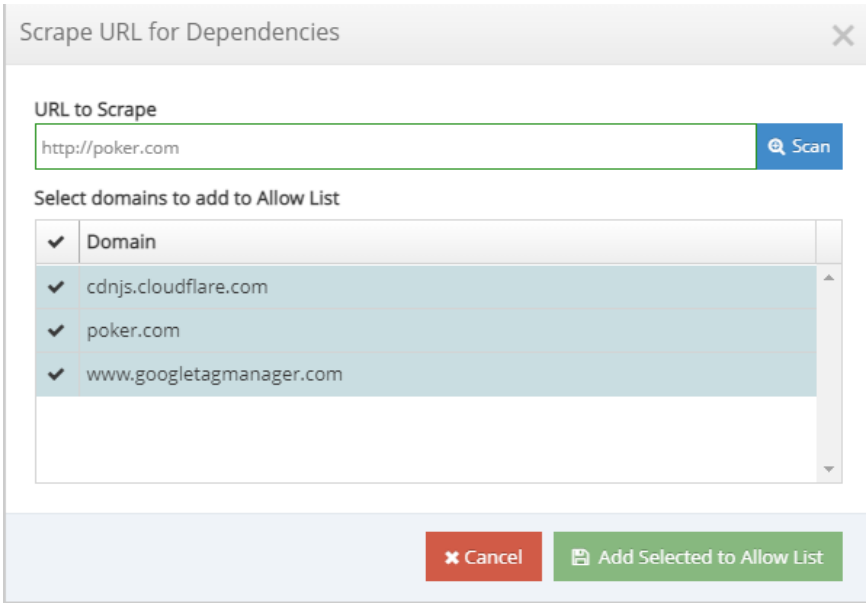
**Step-7: Creating Allow List for website**

- We want to allow **poker.com** to be visited, but continue to disallow other gambling sites,
- Scrape the poker.com site to determine what other sites need to be allowed to have poker.com function
- Click "**Scrape**



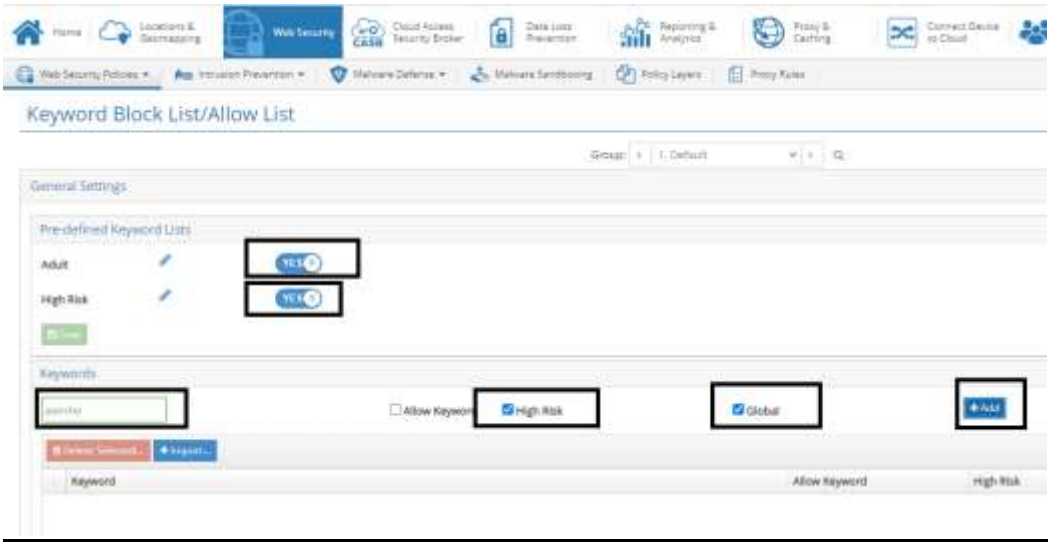

**Step-8: Allow URL Dependencies**

- URL to Scrape, enter "**poker.com**"
- Click "**Scan**"
- Select all domains
- Click "**Add Selected to Allow List**"



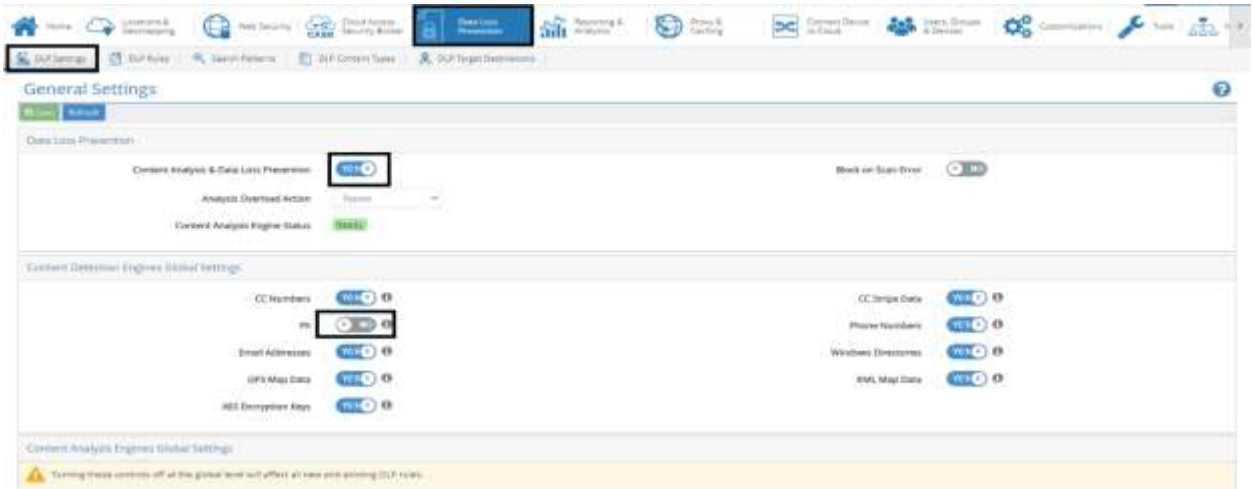
**Step-9: Enable blocking based on Keywords**

- Enable **Adult** and **High Risk** Pre-defined Keyword Lists
- Click "**Save**"
- Add "**poncho**" to keywords, selecting **High Risk** and **Global** prior to clicking "**Add**"



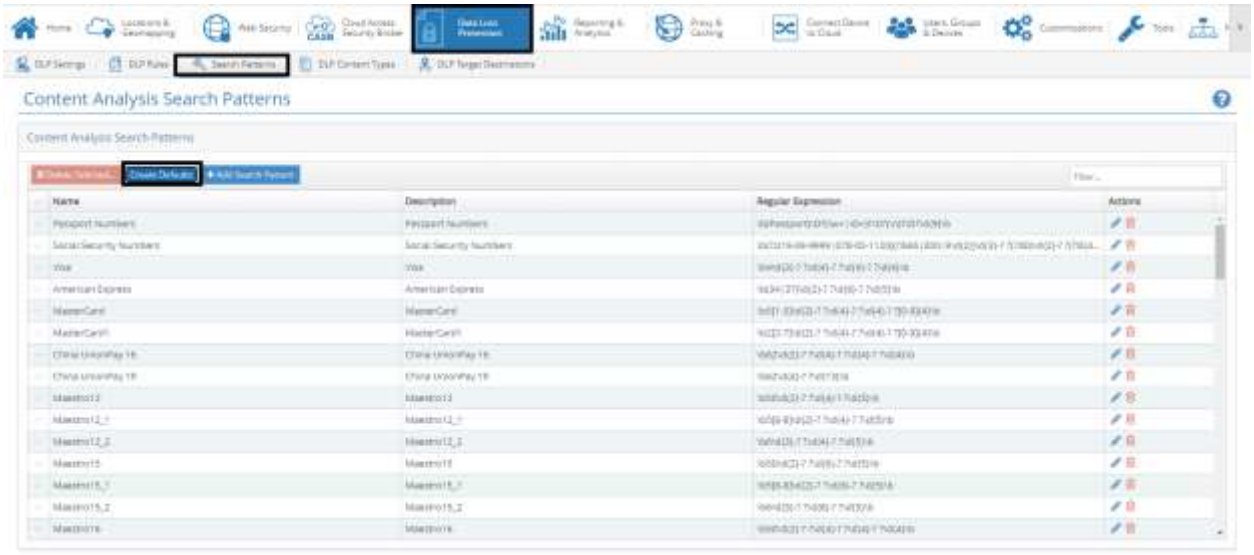

**Step-10: Configure Data Loss Prevention**

- Enable "**Content Analysis & Data Loss Prevention**"
- Enable *all* of the checkboxes (Except "**Block on Scan Error**" and "**PII**")
- Click "**Save**"



**Step-11: DLP Search Patterns**

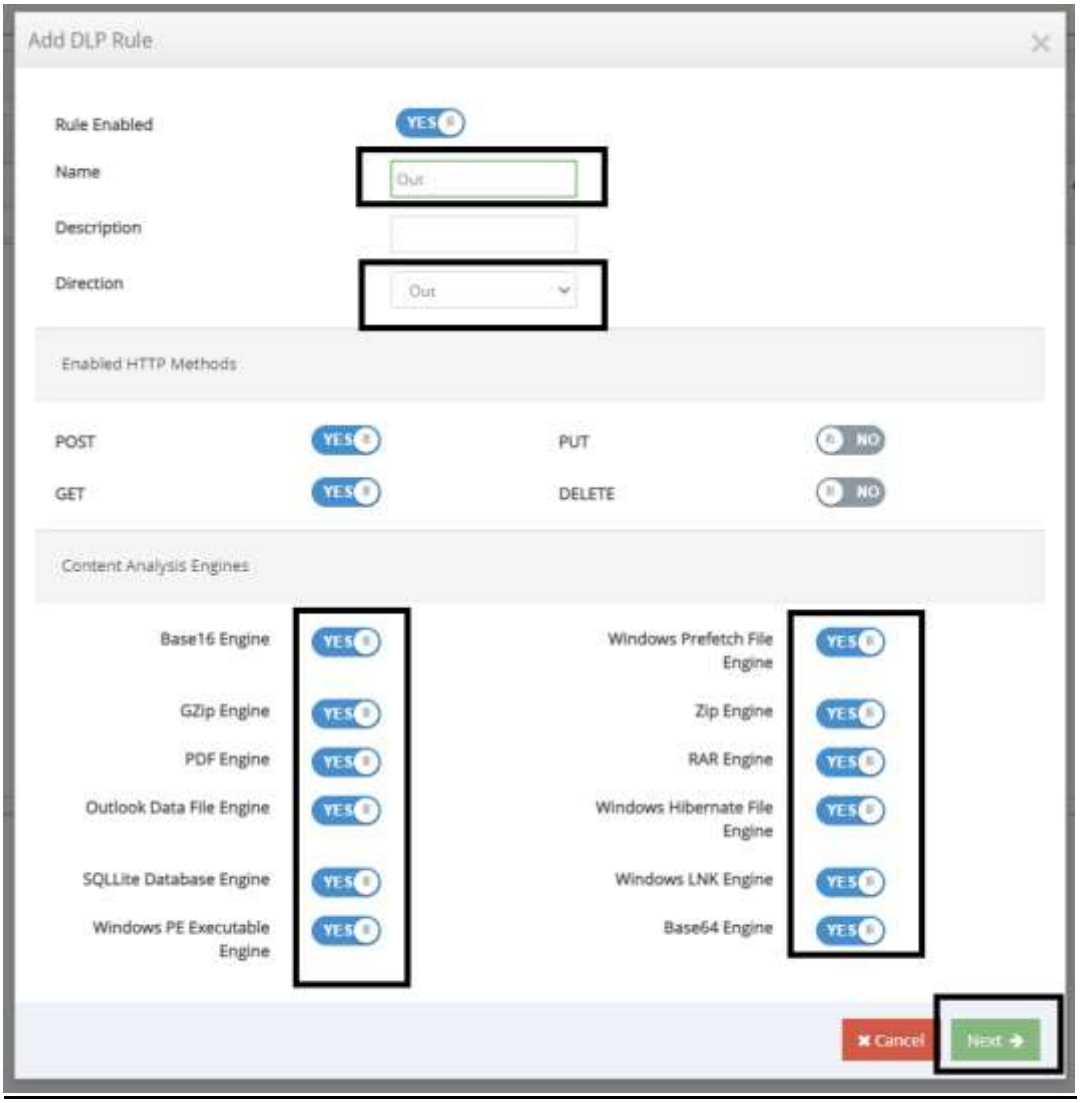
- Click "**Create Defaults**"
- Click "**Create Default Search Patterns**"



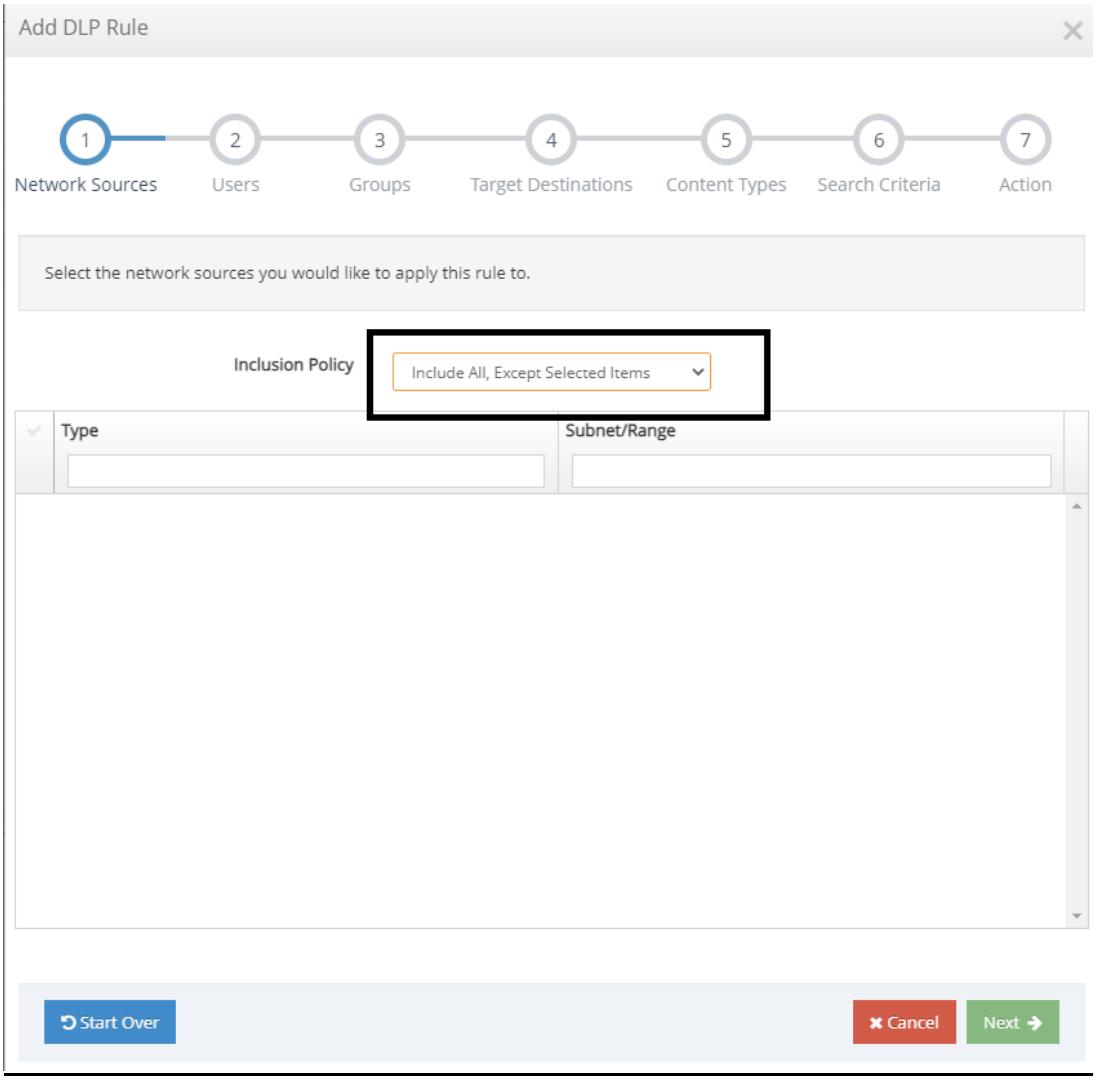

**Step-12: Adding DLP Rules:**

- Click "**Add Rule**"


- Set Name to "**OUT**"
- Set Direction to "**Out**"
- Enable all rules
- Click "**Next**"



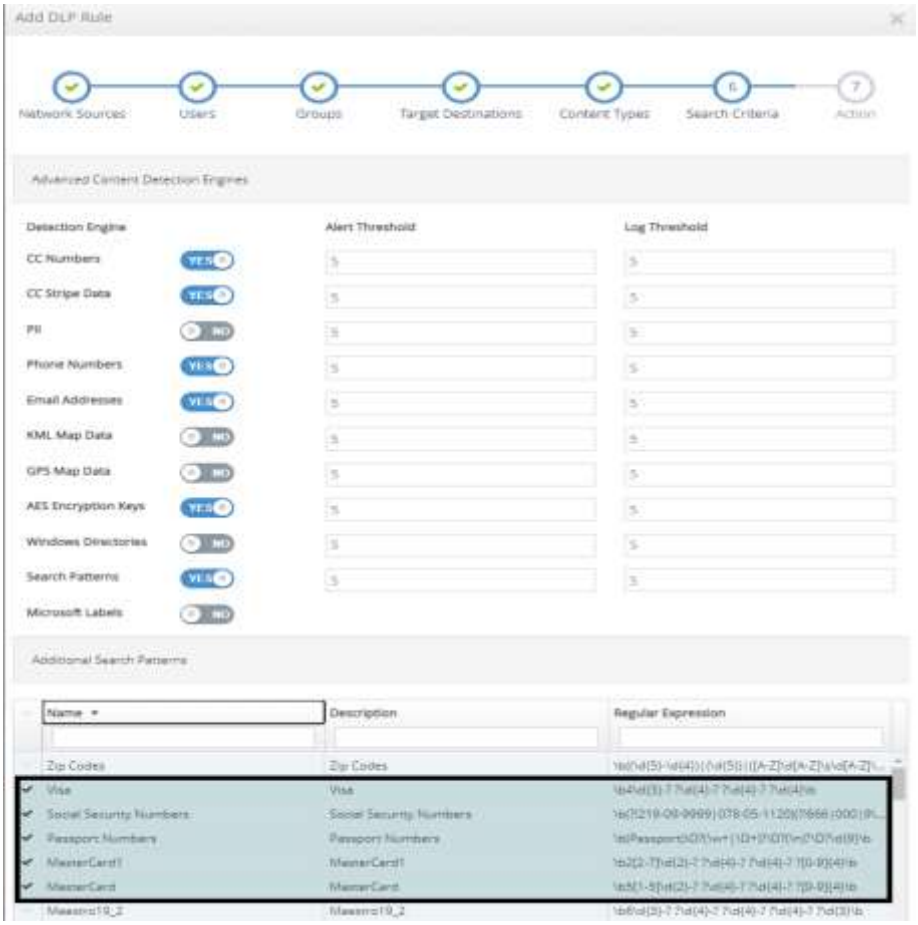

- Change Inclusion Policy to "**Include All, Except Selected Items**"
- Click "**Next**" each time




*Note: Click next till #step-6*

**Configure Search Criteria**

- Disable "**PII**"
- Enable the following Regular Expressions
  - **Visa**
  - **Social Security Numbers**
  - **Passport Numbers**
  - **MasterCard**
  - **MasterCard1**
- Click "**Next**"




**Rule Action Dialog Box**

- Set Action to "**Block**"
- Click "**Save**"