Manual Básico para Administradores del Proxy

Panel de administración> https://proxy.inst.una.py:81/ o https://IP:81/
inst=institución (ing,med,iics,cnc)

1. Creación de usuarios y grupos

1.1 Creación de usuarios

Para la creación de usuarios se debe ir a ***System> Accounts > Users> Add***

Se añade al usuario, entre las opciones, habilitar “Proxy Web User” , y agregarlo a un grupo, por defecto existen 3 que se han creado previamente, no_internet, con_internet, no_rs.

no_internet: No posee acceso a internet, sólo a los correos bajo Gsuite
con_internet: Posee acceso total a internet sin ninguna restricción
no_rs: Posee acceso limitado a internet sin acceso principalmente a redes sociales.

Obs: El usuario debe pertenecer un sólo grupo.

1.2 Creación de grupos

Para la creación de usuarios se debe ir a ***System> Accounts > Groups> Add***

Se añade el nombre del grupo y una descripción del mismo.

La creación de grupos sirven para aplicar sobre ellos filtros de acceso web.

1.3 Cambio de contraseñas

a. Lo puede realizar el administrador ingresando al panel de usuarios.
b. Lo puede realizar el usuario ingresando a la siguiente dirección con su contraseña actual:

https://proxy.inst.una.py:81/

2. Filtro de contenidos y proxy

2.1 Filtro de contenidos

Para acceder al panel de filtro de contenidos debe ir a ***Gateway> Content Filter***

Bloqueo de IPs para el acceso al proxy

Debe ir a ***Gateway> Content Filter and Proxy >Content Filter> Global settings > Banned IPs***

Agregar las IPs que desea bloquear

Administración de las políticas del filtro

Debe ir a ***Gateway> Content Filter Proxy >Content Filter > App policies***

Se puede añadir políticas a un grupo previamente creado en Add

Puede editar la políticas, en “configure policy”, para cada política añadida, donde tenemos las siguientes opciones:

General Settings: Entre sus opciones se puede habilitar el Escaneo de virus(Virus Scan), bloqueo de descargas(Block Downloads) y el bloqueo total(Blanket Block)

Blacklists: Se puede adquirir una lista de bloqueo de distintos tipos de páginas(de Pago)

Banned Sites: Se agrega los sitios que se desea bloquear.

Exception Sites: En caso de que de utilice bloqueo total en la parte de General Settings, aquí se añaden las excepciones.

2.2. Web Proxy

Debe ir a ***Gateway> Content Filter Proxy > Web Proxy Server.***

Autenticación

Por defecto se utiliza *Transparent mode:* Disabled *User authentication:* Enabled.

Obs: Es posible deshabilitar la autenticación usuario en el siguiente modo

Transparent mode: Disabled *User authentication:* Disabled.

Caché

Maximum Cache Size: Es el máximo tamaño del caché del proxy (Por defecto 10Gb)

Maximum Object Size: Es el máximo tamaño del objeto que se puede guardar en el caché(Por defecto 2Gb)

Maximum File Download Size: Aquí se limita el tamaño de los archivos que se pueden descargar(Por defecto 300 Mb)

3. Control de ancho de banda

El ancho de banda general proveído previo acuerdo es limitado por el CNC para el proxy.

Para el control de ancho de banda en las redes internas se puede realizar con el módulo de ancho de banda del clearOS

Para el control de ancho de banda de debe ir a ***Network> Bandwidth Control > Bandwidth Manager.***

El control de ancho de banda se realiza por subredes, por lo que se debe realizar una planificación exhaustiva para la distribución del ancho de banda.

Limitación del Ancho de Banda por subred

Para agregar una subred se debe realizar lo siguiente:

a. Ir a Advanced Rules > Add
b. Rellenar el siguiente formulario:

Rule

Nickname: El nombre de la regla
Direction: Debe se **Flowing to the Network** (No funciona de otra manera)
Interface: El que está por defecto

Match Address

Type: Debe ser **Destination** (No funciona de otra manera)
IpAddress: Se debe poner al subred o la IP a limitar (Ej: 10.0.1.0/24 o 10.0.1.58)

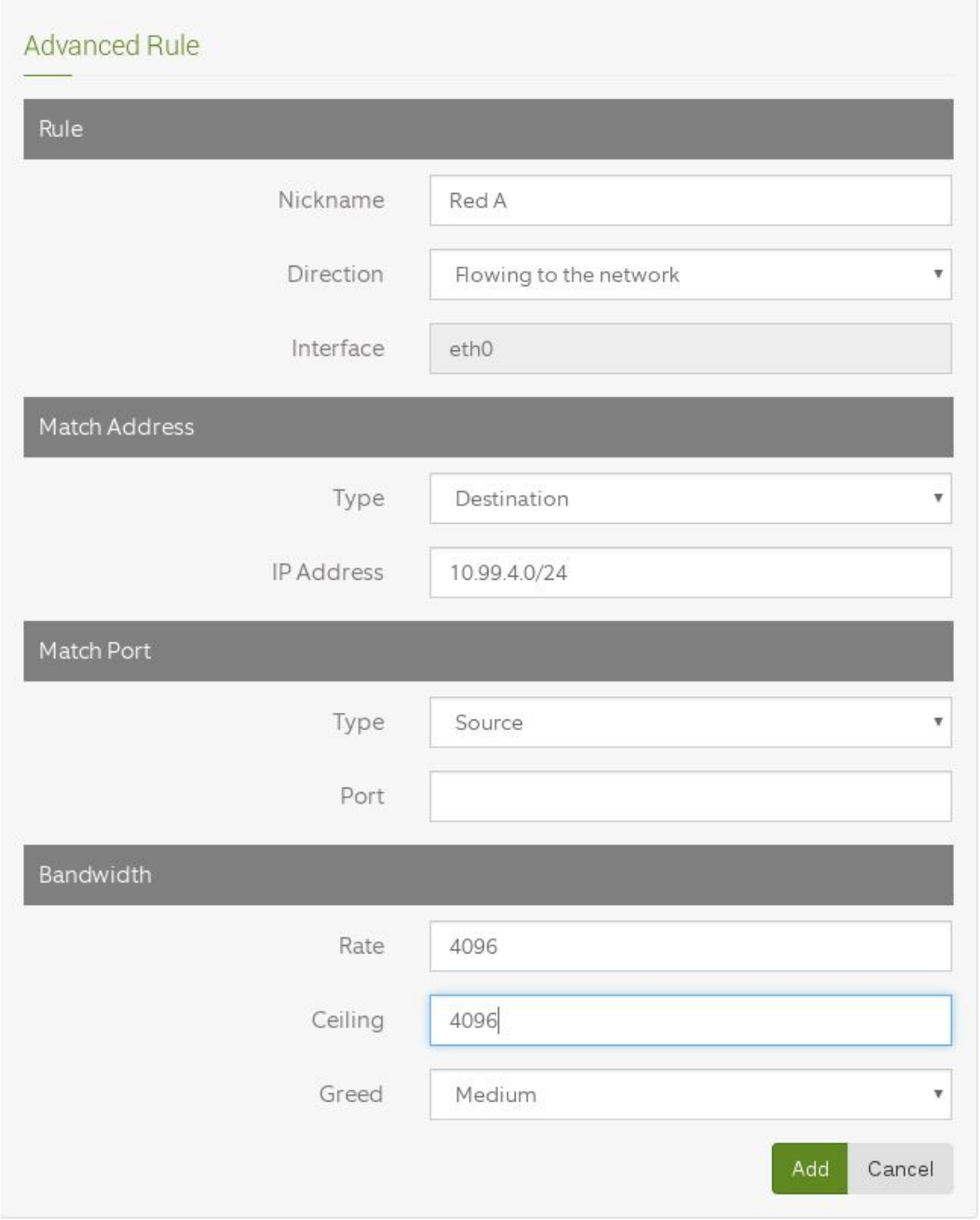
Match Port

Se deja como está.

Bandwitdh

Rate(Kbps): Será el ancho de banda destinado a la subred establecida en el apartado Match Address.
Ceiling(Kbps): Será el ancho de banda reservado para esa red. (Generalmente se establece el mismo valor que Rate)
Greed: Medium

c. Ejemplo (La subred 10.99.4.0/24 limitada a 4 Mbps)



Observaciones:

Para las limitaciones de ancho de banda en toda la red clasificada por subredes, se debe identificar a todas las subredes que utilizan el proxy, debido a que si una o más subredes que utilizan el proxy no está limitada, la misma puede consumir todo el ancho de banda en caso de que se utilicen, es decir las velocidades configuradas no estarán garantizadas.

Si bien la suma del ancho de banda configurada en el módulo puede ser mayor al ancho de banda proveído por el CNC, el ancho de banda total será este último (el proveído

por el CNC), y todas las subredes compartirán el ancho de banda según su utilización en cada subred.

4. Reportes

4.1 Performance and Resources

Bandwidth Viewer: Permite ver el ancho de banda utilizado en tiempo real.

Events and Notifications: Eventos y notificaciones importantes.

Log Viewer: Permite ver los logs del sistemas.

Network Report: Permite ver el historial del Ancho de Banda Total utilizado.

Network Visualizer: Permite observar el ancho de banda por IP utilizado en un corto periodo de tiempo, puede servir para identificar descargas masivas, y bloquear la IP.

Process Viewer: Permite ver los procesos en ejecución.

4.2 User Management

Permite observar las estadísticas de Usuarios, IPs, Sitios y bloqueos de malware del Proxy.