

Políticas de Conectividad

CEDIPAD

DRAFT v5 - Julio 30, 2007

Resumen

En este documento se definen las políticas que debe seguir una Empresa del Ministerio del Comercio Interior para poder conectarse al Centro de Datos MINCIN.

1. Distribución de Direcciones IP

Con el objetivo de homogeneizar las comunicaciones y preparar a la entidad para la migración futura a IPv6 se le asignará a la misma un bloque de 1024 direcciones IP PRIVADAS (172.16.X.Y/22) el cual deberá utilizar en su Red Local.

No debe utilizarse otro grupo de direcciones IP que no sea el asignado por el Centro de Datos así como no se deberá utilizar protocolos de conversión de direcciones como NAT y PAT. El encaminamiento se efectuará de manera estática. El Centro de Datos le proveerá a la empresa una dirección IP para la configuración de la puerta (router) y un gateway predeterminado.

Resumen de direcciones IP:

- La Red 10.0.0.0/8 es utilizada por el servicio PAP de ETECSA.
- La Red 192.168.0.0/16 es utilizada por la red DATOS (INFOCOM) para la interconexión de los routers tanto Frame Relay como IP.
- La Red 172.16.0.0/12 será utilizada por todo el sistema MINCIN.

2. Servicios y Servidores

2.1. Servicios Básicos de Red

Se definen como servicios a nivel de Red los siguientes:

- Servicio de Nombres de Dominio (DNS)
- Servicio de Correo Electrónico (SMTP, POP3, IMAP)
- Validación de usuarios (LDAP)
- Navegación Web (Sin Proxy)
- Antivirus Corporativo (NOD32, Kaspersky, F-Secure)

Es obligatorio que la entidad implemente los servicios anteriores si desea tener servidores propios.

2.2. Dominios y DNS

A las entidades de Ciudad Habana se les asignará un dominio de tercer nivel con la forma empresa.mincin.cu, donde “empresa” determina el nombre o identificador de la misma. En caso que sea una empresa de Provincia, se le asignará un dominio de cuarto nivel con la forma empresa.prov.mincin.cu. Si la empresa cuenta con al menos un servidor de red, en este se deberá configurar un servicio de nombres de dominios (DNS) el cual deberá tener registrado todos los clientes de red (computadoras) de la entidad. Ejemplo: pc-13.empresa.mincin.cu ó pc-13.lan.empresa.mincin.cu donde “pc-13” es el nombre de la computadora y “lan” es un subdominio opcional de quinto nivel definido por la empresa.

La empresa deberá definir los siguientes registros en su servidor DNS:

- ns1.empresa.mincin.cu - Servidor de Nombres de Dominio
- smtp.empresa.mincin.cu - Servicio SMTP
- pop.empresa.mincin.cu - Servicio POP3
- imap.empresa.mincin.cu - Servicio IMAP
- empresa.mincin.cu MX 10 mx0.cinet.cu
- empresa.mincin.cu MX 20 mx1.cinet.cu

Los dos últimos registros (MX) son los servidores de correo electrónico del Centro de Datos, que serán los encargados de gestionar la mensajería. Si no se especifican estos valores, no podrá recibir correo electrónico desde el mundo exterior.

El centro de datos recibirá los correos con destino @empresa.mincin.cu y se los entregará al servidor apuntado por smtp.empresa.mincin.cu.

El servidor DNS de la empresa deberá permitir la transferencia de zonas así como la notificación de cambios hacia el servidor DNS del Centro de Datos (IP: 172.16.0.1). El Centro de Datos se encargará de hacer una copia de la zona y publicarla tanto nacional como internacionalmente según corresponda.

Si la entidad no puede instalar un servidor, el Centro de Datos le brindará todos los servicios necesarios (DNS, Correo, Validación de Usuarios, etc).

Listado de Servidores y Servicios del Centro de Datos:

- mx0.cinet.cu - Servidor de Correo Primario
- mx1.cinet.cu - Servidor de Correo Secundario
- smtp.cinet.cu - Servicio SMTP/Relay (Puerto 25)
- pop.cinet.cu - Servicio POP3 (Puerto 110)
- imap.cinet.cu - Servicio IMAP (Puerto 143)
- correo.cinet.cu - Servicio Web Mail - HTTP (Puerto 80)
- proxy.cinet.cu - Servidor Proxy (Puerto 8080)
- www.cinet.cu - Portal de la Red CINET
- Gateway Predeterminado (IP Routing): 172.16.0.1

3. Cuentas de Usuarios

La empresa deberá publicar el nombre de todos sus usuarios mediante un servicio de directorio (LDAP). El nombre de usuario deberá estar compuesto por varias propiedades con el objetivo de hacerlo único en el sistema. Por ejemplo: “Juan Ramos Espinosa” puede crearse como jrespinosa, juanre o juan.ramos.

La dirección de correos autoritativa para el usuario será usuario@empresa.prov.mincin.cu, sin embargo si el nombre de usuario es único en todo el sistema entonces podrá recibir mensajes también mediante la dirección usuario@mincin.cu. El Centro de Datos se encargará de asociar la cuenta usuario@mincin.cu con usuario@empresa.prov.mincin.cu.

Para publicar las cuentas de todos los usuarios se deberá tener acceso desde el Centro de Datos al puerto TCP 389 (LDAP).

Los servidores LDAP recomendados son:

- Windows 2000/2003 - Active Directory
- UNIX/OpenLDAP

En cualquier caso deben estar visibles los atributos cn, uid y/o mail.

Si la empresa no tiene servidor propio, el Centro de Datos asumirá el control de los usuarios.

En el contenedor “Users” del Directorio se creará un usuario “publico” con una contraseña específica. Esta cuenta será utilizada por el Centro de Datos para sincronizar el Directorio de la Empresa con el Directorio Global de la Red Cinet. El resto de los usuarios de la empresa no se añadirán bajo este contenedor.

Se creará una Unidad Organizativa (Organizational Unit) en el Directorio con el nombre de la empresa, y en la misma es donde se crearán todas las cuentas de usuario de la entidad siguiendo las políticas de nombres determinadas anteriormente.

NOTA: En Active Directory (Windows 2003) hay que rellenar manualmente el campo e-mail para cada usuario (usuario@empresa.mincin.cu) si se utiliza MDaemon como servidor de correo electrónico.

4. Navegación

El Centro de datos permitirá el acceso tanto a Internet como a Cuba según corresponda, vía enrutamiento IP (Sin Proxies). La puerta predeterminada del Centro de Datos es IP: 172.16.0.1.

La empresa deberá implementar un proxy transparente para que los usuarios de red accedan a los recursos de internet/cuba directamente. El control de acceso se efectuará vía IP. Para ello se reservarán IP fijos en el servidor DHCP utilizando la dirección MAC de cada tarjeta de red de los clientes que tengan acceso a Internet. Esto garantizará que la PC siempre tenga una misma dirección IP a pesar de que la misma se configure dinámicamente vía DHCP.

No deberá utilizarse ningún servidor proxy de manera tradicional (Respondiendo peticiones por puerto 8080 o 3128) ya que esto esconde las direcciones IP de los clientes.

Un Proxy Transparente brinda los mismos beneficios que un Proxy Tradicional. La diferencia se encuentra en que un Proxy Transparente filtra las conexiones IP (Acelerándolas utilizando la Cache) pero no las destruye y valida el acceso por IP. Un Proxy Tradicional es un “Puente” que escucha en un puerto específico (8080 o 3128), valida el acceso por usuario, pero esconde todo el tráfico ya que mantiene dos conexiones diferentes: [cliente] < - > [Proxy] < - > [Sitio Web].

Los siguientes programas permiten crear un Proxy Transparente:

- Microsoft ISA Server
- Kerio WinRoute Firewall

- Squid Proxy / Firewall (UNIX)

Se recomienda la utilización del **Kerio WinRoute Firewall** debido a la sencillez de configuración, la poca utilización de recursos y la cantidad de beneficios que brinda. Este software tiene la característica especial que aunque se trabaje con un proxy transparente se valida el acceso por IP y Usuario utilizando el servicio de validación de usuarios Kerberos de Windows.

5. Restricciones

Los servicios y servidores de la empresa deberán velar por el cumplimiento de los siguientes lineamientos:

- No se permitirán mensajes mayores a 1MB.
- No se podrán enviar correos con más de 5 destinatarios. Para cifras mayores se crearán listas de correos en el servidor, minimizando así el tráfico de red.
- Se promoverá el uso de listas y grupos de usuarios.
- No se permitirán los adjuntos potencialmente dañinos (*.EXE, *.COM, *.BAT, etc)
- No se permitirá el SPAM con independencia de su origen.
- Todos los adjuntos deberán viajar compactados utilizando RAR o ZIP.
- No se permitirá el acceso a sitios comprometidos (Pornografía, Contrarrevolución, etc)

CEDIPAD brindará el software y la preparación técnica necesaria con el objetivo de que los administradores de red de la empresa puedan hacer cumplir los puntos anteriores.

6. Control y Estadísticas

El Centro de Datos les facilitará a los clientes el acceso a las estadísticas del uso de los servicios y el estado del consumo del ancho de banda de su enlace (<http://www.cinet.cu>).

La empresa tiene la obligación de conocer y analizar esta información periódicamente y tomar las medidas pertinentes en caso de que se detecte algún uso indebido. También deberán conocer la naturaleza de su tráfico y los protocolos utilizados. Para ello deberá implementar sistemas de registros y bitácoras en la medida de las posibilidades.

7. Aspectos Legales

Cada empresa deberá tener actualizado y en orden los siguientes documentos:

- Licencia de Red
- Plan de Seguridad Informática

Se deberá velar por el cumplimiento y aplicación de las legislaciones vigentes, emitidas por el MIC (Ministerio de Informática y Comunicaciones) y el MINCIN. Para más información diríjase a los siguientes portales:

- <http://www.mic.cu> - Ministerio de Informática y Comunicaciones
- <http://www.cinet.cu> - Centro de datos MINCIN