



Telefónica Argentina

Diseño de OTP en NetScaler

Diseño de OTP en Citrix® NetScaler™

Junio 2014

Preparado Por:

Daniel Castro
Citrix Consulting



Historia de versiones

Versión	Descripción del Cambio	Hecho por	Fecha
0.1	Creación del documento	Fabián Baena.	15/08/2012
0.1.1	Creación del template AGEe	Daniel Castro	01/08/2013
0.2	Modificación OTP	Daniel Castro	13/06/2014

DRAFT

Firmas del entregable

Las firmas a continuación indican el acuerdo entre Telefónica Argentina y Citrix Consulting sobre el contenido del Diseño de OTP en Citrix® NetScaler™.

Telefonica Argentina	Citrix Consulting
Nombre: Martin Giller	Nombre: Daniel Castro
Firma:	Firma:
Título:	Título: Principal Consultant
Fecha:	Fecha: Junio 13 de 2014

Índice

1.1. Resumen Ejecutivo.....	4
1.2. Vista General del Entregable.....	5
2.1. Flujo de Trabajo de la Solución.....	6
2.2. Necesidades que Resuelve este Flujo	7
2.3. Beneficios de la Solución	8
Diseño de la Solución	9
3.1. Diagrama de Comunicación	10
3.2. Configuración de NetScaler.....	12
3.2.1. Expresiones	12
3.2.2. Reponder.....	12
3.2.3. Explicación Virtual Servers.....	13
3.2.3.1. NetScaler Gateway	13
3.2.3.2. Load Balance Virtual Server	14
3.2.3.3. AAA-TM Virtual Server.....	14
3.3. Sevidor RADIUS OTP	15
3.3.1. Codigo Servidor.....	17
Operaciones.....	20
4.1. Mantenimiento	21
4.2. Soporte.....	21
Apéndices	22
5.1. Apéndice A – Direccionamiento IP y Reglas de Firewall.....	23

DRAFT

1. Vista General

1.1. Resumen Ejecutivo

Telefónica Argentina tiene una solución de NetScaler Gateway que está siendo usada, primordialmente, por empleados y proveedores. Esta solución de NetScaler Gateway hace énfasis en la seguridad de la plataforma y por ello en la actualidad hace uso de un segundo factor de autenticación llamada MOVIID. Este segundo factor de autenticación es una solución hecha a la medida, que interactúa directamente con la planta telefónica para la generación del One Time Password. MoviID es una solución antigua que desean sea remplazada por una solución de OTP que envíe el token de autenticación por medio de SMS, es por esto que Telefónica Argentina le ha pedido a Citrix Consulting que haga un desarrollo a la medida que permita que NetScaler tenga una nueva solución OTP, facilitando así el segundo factor de autenticación.

1.2. Vista General del Entregable

Este documento de diseño de OTP para NetScaler es el resultado de la colaboración con el área de Seguridad Estratégica de Telefónica Argentina y Citrix Consulting.

Basado en las discusiones colaborativas, la arquitectura descrita en este documento representa las decisiones de diseño hechas en conjunto con Citrix Consulting durante el transcurso de este encuentro.

Este diseño arquitectónico está organizado de la siguiente manera:

Sección	Temas cubiertos
Vista General Ejecutiva y Diseño Arquitectónico	Esta sección provee una vista general del proyecto, incluyendo temas de diseño. Se detallan los fundamentos de arquitectura del diseño de NetScaler.
Flujo de Trabajo del Desarrollo	Se provee una vista desde la perspectiva del usuario y como este interactúa con los componentes.
Diseño de la Solución	Detalle de cada uno de los componentes que se involucran en la solución.
Código de la Solución	Muestra el código fuente del componente Servidor

Sección	Temas cubiertos
Mantenimiento	Dependencias e Instrucciones de instalación y los diferentes archivos involucrados.
Soporte	Detalla el proceso de soporte, el proceso de escalación con Citrix Consulting.

Flujo de Trabajo de la Solución

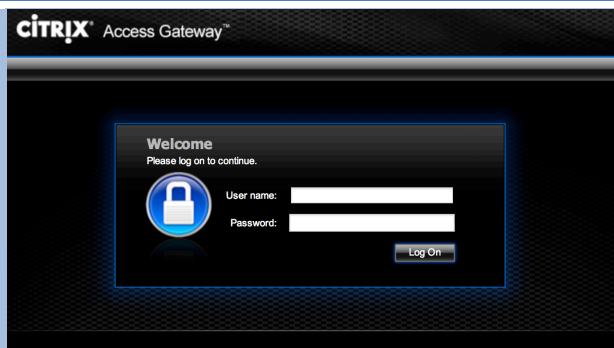
Desde la perspectiva de usuario, el flujo de trabajo inicia desde el momento en el que el usuario escribe la URL del sitio de teletrabajo que desea utilizar. A partir de la primera petición HTTP el NetScaler toma control del flujo y envía al usuario a la pantalla de autenticación de sus credenciales de Active Directory.

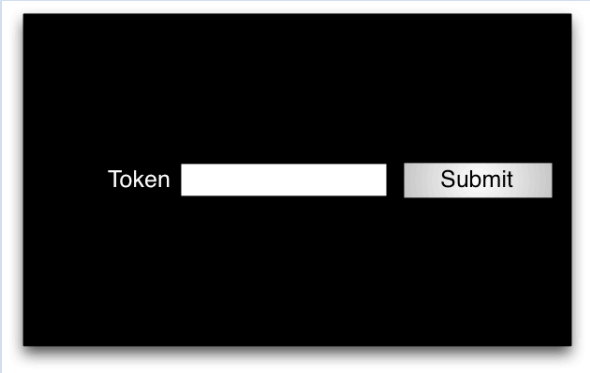
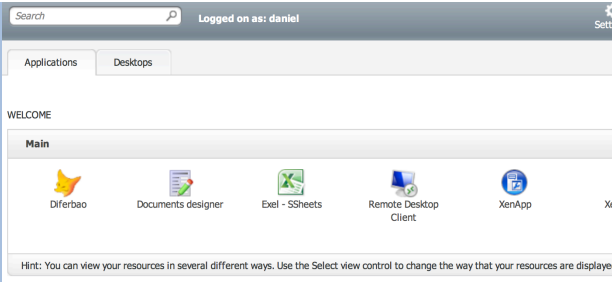
Una vez el usuario ha acreditado sus credenciales, se inicia el proceso de emisión del token vía SMS, este proceso sucede del lado del servidor y no está bajo el control del usuario.

A continuación al usuario se le presenta una pantalla en la que debe ingresar su token para el segundo factor de autenticación y presionar continuar.

Posteriormente el usuario realiza el proceso de autenticación automático sobre el sitio de teletrabajo que había seleccionado inicialmente.

Las siguientes son las pantallas visibles por el usuario:

Paso	Pantalla	Comentarios
1		<p>Es la pantalla por defecto de inicio de sesión para los usuarios. La URL que escribe inicialmente el usuario es usada para hacer SSO en el paso 2.</p> <p>Una vez un usuario ha iniciado sesión, el sistema genera el token y lo envía por medio de SMS.</p> <p>TODO: Incluir un dropdown del</p>

		dominio. Esto debe ser usado en el Paso 2 para hacer SSO también en el dominio apropiado.
2		<p>Es la pantalla post-autenticación, en este punto el sistema ya envió el SMS con el token, y el usuario tan solo debe ingresarlo en el campo para continuar al Web Interface.</p> <p>Si falla en la autenticación del token, se debe enviar a esta misma pantalla mediante una serie de redirecciones http. Al fallar 3 intentos, la sesión se vence y debe esperar a que el token venza para solicitar uno nuevo.</p> <p>En caso de ser un dispositivo móvil, se presenta una pagina informativa con el tiempo de expiración aproximado del token; Por ejemplo: "Su token ha sido enviado por SMS y vence a las XX:XX:XX". Adicionalmente, no se permite interacción con el usuario.</p>
3		Una vez el usuario ingresa el token y el sistema lo valida se realiza el proceso de inicio de sesión en el Web Interface

1.4. Necesidades que Resuelve este Flujo

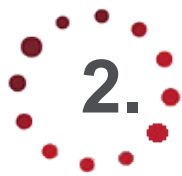
Desde la perspectiva de usuario, la solución que desea implementar Telefónica Argentina simplifica el proceso actual de autenticación al cual son sometidos los usuarios, sin

embargo, no disminuye el nivel de seguridad que provee la solución actual. Este desarrollo sustituye MoviID por completo.

1.5. Beneficios de la Solución

La solución actual de MoviID requiere que los usuarios llamen a un numero telefónico especial que solo puede ser discado desde la Argentina impidiendo que los usuarios internacionales de Telefónica hagan uso de la plataforma. La solución actual de SMS puede ser consultada desde cualquier parte del mundo, siempre y cuando el usuario tenga habilitado su roaming internacional.

DRAFT



2. Diseño de la Solución

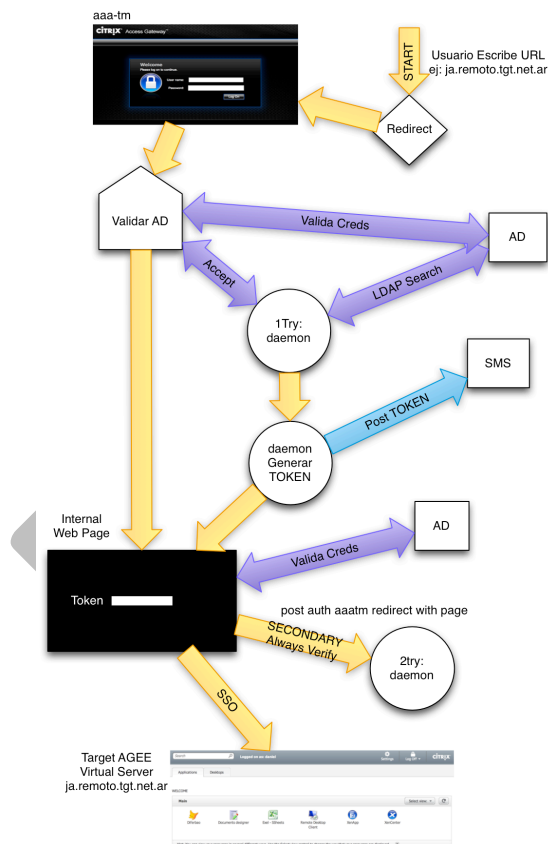
1.6. Diagrama de Comunicación

La solución a la medida de OTP para NetScaler tiene dos capas principales que permiten el correcto flujo del usuario por las diferentes etapas. Las dos capas son:

- Reglas de NetScaler y Virtual Servers
- Servidor Radius

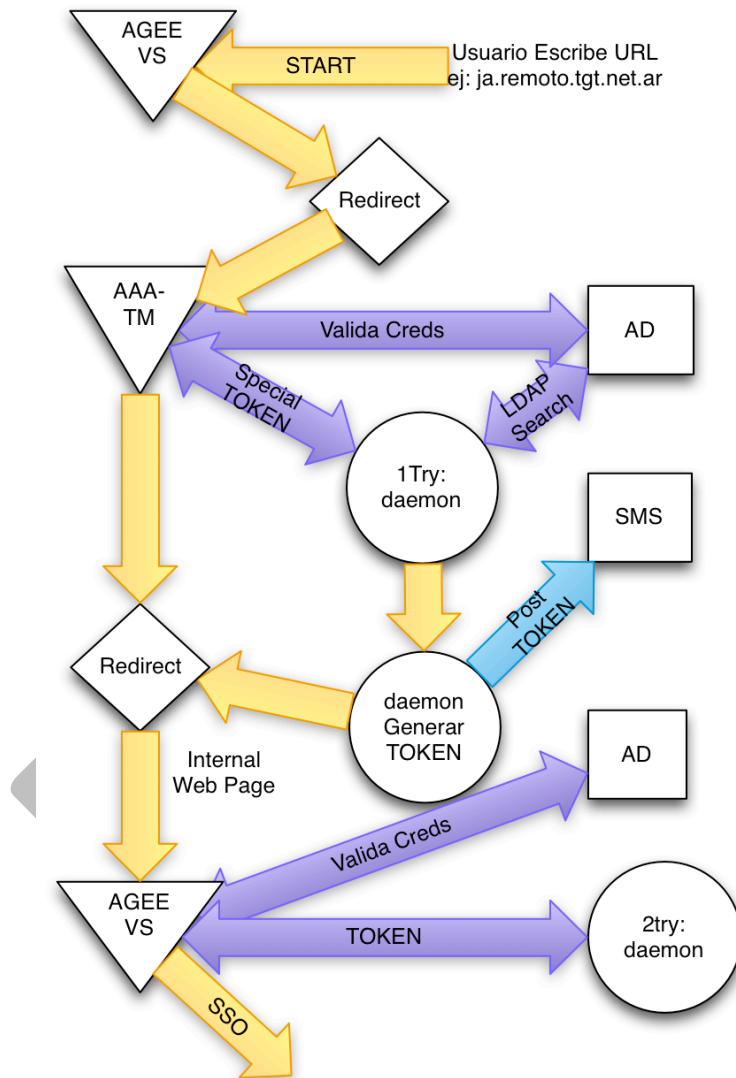
Las reglas del NetScaler corresponden a todas las políticas y acciones de la funcionalidad Responder, que permiten guiar al usuario entre los diferentes pasos. Los Virtual Servers son las diferentes direcciones IP con las que interactúa el usuario a lo largo del proceso de autenticación.

El siguiente diagrama muestra el flujo de trabajo y todos sus componentes:



Como se puede ver en el diagrama anterior, las pantallas son los únicos puntos de contacto visibles para el usuario, las redirecciones (objeto Rombo) interactúan con el usuario pero no hay control directo sobre la redirección. Los objetos en forma de círculo corresponden al componente Servidor y los objetos en forma de Cuadrado son componentes externos.

El mismo proceso visto desde la perspectiva de NetScaler se muestra en el siguiente flujo:



1.7. Configuración de NetScaler

A continuación se muestran las diferentes configuraciones necesarias para el correcto funcionamiento.

Expresiones

Para poder generar el contenido dinámico de manera adecuada es necesaria la utilización de una serie de expresiones, esto permite realizar llamadas recursivas en el sistema:

Nom bre	Expresión	Explicación
STEP2_BASIC	<pre>\ "<html><head><META HTTP-EQUIV=\\\\"Content-Type\\\\"CONTENT=\\\\"text/html; charset=UTF-8\\\\">\"+\n<style type=\\\\"text/css\\\\"></style>\n</head>\"+\n<body>\n<form action=\\\\"https://\"+http.REQ.URL.QUERY.VALUE(\"url\")+\n\"/cgi/login\\\\" method=\\\\"post\\\\">\n<input type=hidden name=login value=\\\\"\"+http.REQ.USER.NAME +\\\\"\\\\">\n<input type=hidden name=passwd value=\\\\"\"+http.REQ.USER.PASSWD+\\\\"\\\\">\n\"+\n<input id=\\\\"Continue\\\\" type=\\\\"submit\\\\" value=\\\\"Continue\\\\">\n</form>\"+\n</body></html>\""</pre>	<p>Esta expresión contiene la pagina dinámica que se le presenta al usuario después de la autenticación, en esta el usuario debe ingresar el token para poder continuar el proceso.</p> <p>Esta página aún requiere de personalización para Telefónica</p>

Reponder

Esta funcionalidad permite enviar al usuario a destinos específicos basados en políticas, también permite presentar contenido basado en políticas. A continuación se muestran las acciones configuradas en le sistema:

Nombre Acción	Tipo de Acción	Respuesta
START_GOTO_STEP_1	Redirect	"\"http://auth.remoto.tgt.net/start?url=\"+http.REQ.HOSTNAME"

STEP2_PAGE_RESP	Respond With	"\"HTTP/1.1 200 OK\nCache-Control: private, max-age=0\"+\nContent-Type: text/html; charset=utf-8\nContent-Length: \"+STEP2_BASIC.LENGTH+\n\\r\\n\\r\\n\\n\"+STEP2_BASIC"
STEP2_MOV_PAGE_RESP	Respond With HTML	TODO, página de móviles

A continuación se muestran las políticas configuradas en el sistema:

Nombre Política	Regla	Acción	Bind
POL_START_GOTO_STEP_1	"http.REQ.HOSTNAME.EQ(\"agee.test.com\")&&(http.REQ.URL.EQ(\"/\") http.REQ.URL.ENDSWITH(\"index.html\"))"	START_GOTO_STEP_1	GLOBAL OVERRIDE
POL_STEP2_PAGE_RESP	"http.REQ.URL.STARTSWITH(\"/start\")"	STEP2_PAGE_RESP	Virtual Server
POL_STEP2_MOV_PAGE_RESP	"http.REQ.URL.STARTSWITH(\"/start\")&&(http.REQ.header(\"User-Agent\").CONTAINS(\"Android\") http.REQ.header(\"User-Agent\").CONTAINS(\"IPhone\"))"	STEP2_MOV_PAGE_RESP	Virtual Server

Explicación Virtual Servers

Existen tres tipos de virtual servers en esta solución con una función específica, teniendo en cuenta la configuración actual y los requerimientos de la plataforma de Telefónica se explica cada tipo de virtual server y los cambios que requiere para que la solución de OTP funcione correctamente.

NetScaler Gateway

Estos virtual servers ya se encuentran creados en la plataforma de Telefónica, requieren de un cambio puntual en la configuración de Autenticación Secundaria de MoviID a la nueva solución de OTP.

Load Balance Virtual Server

Este virtual server no se encuentra creado y es necesario asignarle el FQDN correspondiente que debe ser tipo SSL. En este virtual server van a estar asignadas las políticas de responder y autenticación que permite capturar el flujo de transacciones del usuario y forzarlo a autenticarse ante la funcionalidad de AAA-TM para solicitar su Token y su posterior validación. Este virtual server puede no tener ningún contenido, pero se recomienda que tenga un monitor cuya respuesta siempre sea positiva. Se debe habilitar la funcionalidad de autenticación y usar el FQDN correspondiente al Virtual server de AAA-TM.

AAA-TM Virtual Server

Este virtual server tiene características especiales en cuanto a que requiere la utilización de autenticación de doble factor, pero para el campo de password secundario no le solicita un dato al usuario, pero el contrario envía un campo de password secundario con un valor especial lo que le indica al servidor OTP que debe generar un token para el usuario que está en proceso de autenticación.

Para poder lograr lo anterior es necesario modificar la pagina donde se le solicitan las credenciales al usuario, esta página se encuentra en /netscaler/ns_gui/vpn/index_tm.html. En esta página se debe incluir el sistema de dropdown para dominio y se debe modificar también la funcion JavaScript que crea el campo secundario de password, para que al hacerlo no sea editable para el usuario, se recomienda usar la siguiente modificación a la función:

```
function ns_showpwd()
{
    var pwc = ns_getcookie("pwcount");
    document.write('<TR><TD align=right style="padding-right:10px;white-space:nowrap;"><SPAN
class=CTXMSAM_LogonFont>' + _("Password"));
    if ( pwc == 2 ) { document.write('&nbsp;1'); }
    document.write('</SPAN></TD>');
    document.write('<TD colspan=2 style="padding-right:8px;"><input
class=CTXMSAM_ContentFont type="Password" title="' + _("Enter password") + "' name="passwd"
size="30" maxlength="127" style="width:100%;"></TD></TR>');
    if ( pwc == 2 ) {
        document.write('<TR><TD align=right style="padding-right:10px;white-space:nowrap;"><SPAN
class=CTXMSAM_LogonFont>' + _("Password2") + '</SPAN></TD> <TD colspan=2 style="padding-
right:8px;"><input type=hidden name="passwd1" value=""></TD></TR>');
```

}

1.8. Sevidor RADIUS OTP

Esta solución se basa en que el NetScaler solo puede comunicarse con el Servidor OTP por medio del protocolo RADIUS, basados en esto se ha creado un software que corre en el Kernel FreeBSD del NetScaler como un proceso iniciado por el sistema.

Para que dicho software pueda correr es necesario cumplir con una serie de dependencias de software, la siguiente es la lista de librerías que deben ser instaladas en el sistema:

- mach/
 - auto/Net /
 - Gen/
 - EOF.al
 - FETCH.al
 - GETC.al
 - Gen.bs
 - Gen.so
 - PRINTF.al
 - READ.al
 - READLINE.al
 - RECV.al
 - STORE.al
 - TIEHANDLE.al
 - TIESCALAR.al
 - WRITE.al
 - _findxopt.al
 - _getxopt.al
 - _setxopt.al
 - accept.al
 - autosplit.ix
 - bind.al
 - delparam.al
 - didlisten.al

- fcntl.al
- fhvec.al
- fileno.al
- format_addr.al
- format_local_addr.al
- format_remote_addr.al
- getfh.al
- getlines.al
- getropt.al
- getsopt.al
- ioctl.al
- listen.al
- new_from_fh.al
- select.al
- sendto.al
- setdebug.al
- setparam.al
- setropt.al
- setsopt.al
- unbind.al
- Inet
 - Autosplit.ix
 - Bind.al
 - Setdebug.al
 - Unbind.al
- UDP
 - _setbuf_unbuf.al
 - autosplit.ix
 - PRINT.al
 - READLINE.al
- UNIX
 - autosplit.ix
 - bind.al
 - setdebug.al
- Net/
 - Gen.pm

- Inet.pm
- TCP/
 - Server.pm
- TCP.pm
- UDP.pm
- UNIX/
 - Server.pm
- UNIX.pm
- MD5.pm
- RADIUS/
 - Dictionary.pm
 - Packet.pm

Al copiar las anteriores dependencias a la carpeta: /usr/local/lib/perl5/site_perl/5.8.8/ se puede ejecutar el servidor. Lo anterior se encuentra almacenado en archivo Tar comprimido en la carpeta /var y se descomprime y ejecuta de manera automática por un script de inicio en el NetScaler.rc.

Las líneas correspondientes en el archivo RC son:

- tar -zxf radius.tar.gz -C /
- /var/captcha/radius.pl &

Codigo Servidor

A continuación se presenta el código del servidor en su estado a la fecha:

```
#!/usr/local/bin/perl -w

use RADIUS::Dictionary;
use RADIUS::Packet;
use Net::Inet;
use Net::UDP;
use Fcntl;
use strict;

# This is a VERY simple RADIUS authentication server which responds
# to Access-Request packets with Access-Accept. This allows anyone
# to log in.
```

```

my $secret = "mysecret"; # Shared secret on the term server

# Parse the RADIUS dictionary file (must have dictionary in current dir)
my $dict = new RADIUS::Dictionary "dictionary"
    or die "Couldn't read dictionary: $!";

# Set up the network socket (must have radius in /etc/services)
my $s = new Net::UDP { thisservice => "radius" } or die $!;
$s->bind or die "Couldn't bind: $!";
$s->fcntl(F_SETFL, $s->fcntl(F_GETFL,0) | O_NONBLOCK)
    or die "Couldn't make socket non-blocking: $!";

# Loop forever, receiving packets and replying to them
while (1) {
    my ($rec, $whence);
    # Wait for a packet
    my $nfound = $s->select(1, 0, 1, undef);
    if ($nfound > 0) {
        # Get the data
        $rec = $s->recv(undef, undef, $whence);
        # Unpack it
        my $p = new RADIUS::Packet $dict, $rec;
        if ($p->code eq 'Access-Request') {
            # Print some details about the incoming request (try ->dump here)
            print $p->attr('User-Name'), " logging in with password ",
                $p->password($secret), "\n";
            # Create a response packet
            my $rp = new RADIUS::Packet $dict;
            $rp->set_code('Access-Accept');
            $rp->set_identifier($p->identifier);
            $rp->set_authenticator($p->authenticator);
            # (No attributes are needed.. but you could set IP addr, etc. here)
            # Authenticate with the secret and send to the server.
            $s->sendto(auth_resp($rp->pack, $secret), $whence);
        }
        else {
            # It's not an Access-Request
            print "Unexpected packet type recieved.";
            $p->dump;
        }
    }
}

```

}

DRAFT



3. Operaciones

1.9. Mantenimiento

El archivo otp.tar.gz contiene todos los archivos necesarios para correr el servidor, en caso de falla el principal síntoma será la negación de acceso a todos los usuarios. Esto se debe a que el sistema va a negar las peticiones de Token. Este debe auto instalarse tras cada reinicio de las máquinas sin necesidad de interactuar con el administrador. Es necesario verificar que el archivo /nsconfig/netscaler.rc contiene las líneas descritas en

Si el sistema no está entregando los mensajes de texto con el token, puede deberse a un problema en el Gateway de SMS, o a que la configuración para envío de SMS ha cambiado. Si lo segundo ha sucedido es necesario examinar el código del servidor y cambiar los parámetros del POST en la sección de SMS.

El servidor deja una bitácora en /var/log/token_radius.log donde se guardan el número telefónico al cual se le envió el token, el usuario y la respuesta del Gateway SMS. En otra entrada verá el acceso al sistema por parte del usuario, es decir cada ingreso debe tener dos entradas.

Para deshabilitar el sistema, se deben quitar las políticas de autenticación secundarias y se debe quitar del nivel global la política de responder POL_START_GOTO_STEP1. Con esas dos operaciones el NetScaler permite el ingreso directo de los usuarios al Virtual Server de NetScaler Gateway y la autenticación puede proceder contra Active Directory.

1.10. Soporte

El soporte de primer nivel siempre estará a cargo de DWS, por medio de la documentación y transferencia de conocimiento en sitio al personal de soporte de DWS que estará en la capacidad de atender pequeños incidentes sobre la plataforma.

En caso de que Telefónica requiera de hacer una actualización de su plataforma más allá de la versión 10.1 se debe coordinar con Citrix Systems una visita programada para poder estudiar el impacto que dicha actualización pueda tener sobre el sistema.

4. Apéndice

1.11. Apéndice A –

Citrix NetScaler

DRAFT

DRAFT

The copyright in this report and all other works of authorship and all developments made, conceived, created, discovered, invented or reduced to practice in the performance of work during this engagement are and shall remain the sole and absolute property of Citrix, subject to a worldwide, non-exclusive license to you for your internal distribution and use as intended hereunder. No license to Citrix products is granted herein. Citrix products must be licensed separately. Citrix warrants that the services have been performed in a professional and workman-like manner using generally accepted industry standards and practices. Your exclusive remedy for breach of this warranty shall be timely re-performance of the work by Citrix such that the warranty is met. THE WARRANTY ABOVE IS EXCLUSIVE AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE WITH RESPECT TO THE SERVICES OR PRODUCTS PROVIDED UNDER THIS AGREEMENT, THE PERFORMANCE OF MATERIALS OR PROCESSES DEVELOPED OR PROVIDED UNDER THIS AGREEMENT, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR AGAINST INFRINGEMENT. Citrix' liability to you with respect to any services rendered shall be limited to the amount actually paid by you. IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY HEREUNDER FOR ANY INCIDENTAL, CONSEQUENTIAL, INDIRECT OR PUNITIVE DAMAGES (INCLUDING BUT NOT LIMITED TO LOST PROFITS) REGARDLESS OF WHETHER SUCH LIABILITY IS BASED ON BREACH OF CONTRACT, TORT, OR STRICT LIABILITY. Disputes regarding this engagement shall be governed by the internal laws of the State of Florida.