

Configuración de NAT en los Cisco Adaptive Security Appliances (ASAs) a partir de versiones 8.3

Experto:

Julio Carvajal Segura

Martes 4 de agosto del 2012

Comunidad de Soporte de Cisco

Webcast en vivo

- El experto del día de hoy es **Julio Carvajal**
- Ahora puede hacerle sus preguntas sobre La Configuración NAT en los Cisco ASA's.



Gracias por su asistencia el día de hoy

La presentación incluirá algunas preguntas a la audiencia.

Le invitamos cordialmente a participar activamente en las preguntas que le haremos durante la sesión





Copia de la presentación

Si desea bajar una copia de la presentación de hoy, diríjase al enlace indicado en el chat o use la siguiente dirección:

<https://supportforums.cisco.com/docs/DOC-26813>



Primera pregunta a la audiencia

¿Qué tan familiarizado está con el NAT a partir de 8.3?

- a) No estaba consciente de que hubo cambios**
- b) Sé que cambió drásticamente pero no lo he utilizado**
- c) Lo utilizo día a día en prácticas.**
- d) Lo tengo corriendo en producción.**

¡ Ahora puede realizar sus preguntas al panel de expertos!

Use el panel de preguntas y respuestas (Q&A) para preguntar a los expertos ahora. Ellos empezarán a responder.





Configuración de NAT en los Cisco Adaptive Security Appliances (ASAs) a partir de versiones 8.3

Julio Carvajal Segura

CCSP

Martes 4 de setiembre del 2012

Agenda

- **Requisitos para migrar a 8.3**
- **Orden en el Nat (8.2 vs 8.3)**
- **Tipos de Nat**
- **Cambios en las listas de acceso**
- **Laboratorio de Nat y listas de acceso**
- **Introducción a SLA**
- **Configuración de SLA**

Requisitos para migrar a 8.3



Requisitos para migrar a 8.3

- Comando Nat-Control (versiones 6,7 y 8.3)
- Memoria RAM

ASA 5505	512MB
ASA 5510	1024MB
ASA5520	2048MB
ASA5540	2048MB
5550,5580,etc	No necesaria

Orden de NAT en 8.3



Orden de NAT 8.2 VS 8.3

- 8.2:
 - Nat 0 con lista de acceso (Excepción de Nat)
 - Xlate
 - Nat estático o PAT estático
 - Policy NAT
 - Nat Dinámico
- 8.3:
 - Doble Nat (Twice Nat)
 - Auto Nat
 - Después del Auto Nat (After Auto Nat)

Tipos de NAT

Auto Nat, Doble Nat (Twice Nat) , Después del auto Nat (After Auto)



Auto Nat

- La regla de NAT es incluida dentro de un objeto.
- Puede ser dinámico o estático

```
(config)# Object network PC_1
```

```
(config-network-object)# Host 192.168.12.10
```

```
(config-network-object)# Nat (inside,outside) static 4.2.2.2
```

Doble Nat (Twice Nat)

- Toma en cuenta para la traducción, tanto el origen del tráfico, como el destino de este.
- Permite realizar lo que antes se conocía como *Policy Nat* en una sola línea.

```
(config)# Nat (inside,outside) source static objeto_1 Objeto_2 destination static objeto_3 objeto_3
```

```
(config)# Nat (inside,dmz) source dynamic red_interna_1 Objeto_5 destination static objeto_4 objeto_3
```

Después del Auto Nat (After Auto)

- Permite configurar un doble nat (*twice nat*) y enviarlo al último puesto en lo de las reglas nat.

(config)# Nat (inside,outside) after-auto source dynamic any interface

Problemas más comunes con Nat en 8.3

- 1) El determinar si al usar servicios , el objeto debe ser de origen o destino. Basarse en la interfaz asociada al dispositivo que se espera alcanzar.

```
Object service SMTP
```

```
    service tcp source eq 25
```

```
Object service HTTP
```

```
    service tcp destination eq 80
```

- 2) El tener reglas generales sobre reglas específicas va a ocasionar que éstas últimas nunca sean tomadas en cuenta.

```
nat (inside,outside) source dynamic any interface
```

```
nat (inside,outside) source static HTTP_Privada HTTP_Publica
```

Problemas más comunes con Nat en 8.3

- 3) Uso del Any como interfaz en las traducciones:

Utilizar esta palabra nos puede llegar a ocasionar problemas de enrutamiento o hasta problemas con el mecanismo de *proxy-arp*.

```
Nat (any,outside) source dynamic any interface
```

- 4) Uso de la palabra *unidirectional* en las traducciones en los doble nat

Este comando va a hacer que sólo se permita tráfico del origen al destino, la conexión nunca va a poder ser iniciada desde la otra interfaz. Este error se ve normalmente al hacer la mejora del OS con respecto a las reglas de Nat 0

```
nat (inside,outside) source static LAN LAN destination static Remote  
Remote unidirectional
```

Verificación de las reglas de Nat

- -Show Xlate:

23 in use, 47 most used

TCP PAT from inside:10.10.33.10 80-80 to outside:10.198.28.33 80-80

flags sr idle 4:35:13 timeout 0:00:00

TCP PAT from inside:10.10.33.10 3389-3389 to outside:60.60.60.53 3389-3389

- -Show nat:

Manual NAT Policies (Section 1)

1 (inside) to (outside) source static HTTP_Server interface-ip service Port80 Port80

translate_hits = 0, untranslate_hits = 1

Auto NAT Policies (Section 2)

1 (inside) to (outside) source static FTP_server interface service tcp ftp ftp

translate_hits = 0, untranslate_hits = 33

Segunda Pregunta a la audiencia

¿Qué tanto conoce la sintaxis de las listas de acceso en la versión de software 8.3?

- a) No estaba anuente a un cambio en la sintaxis**
- b) Conocimiento teórico**
- c) He trabajado con ellas muy pocas veces.**
- d) Trabajo con ellas día a día**

Listas de acceso



Estructura de las listas de acceso (ACL)

- **Cambio en el orden de operaciones del ASA:**
 - A partir de 8.3 el ASA verificará primero las operaciones de NAT y posteriormente las listas de acceso.
 - A partir de 8.3 se debe de apuntar a la IP interna de los dispositivos en la red.

Trafico a través del ASA

- Tráfico de una interfaz con un nivel de seguridad mayor hacia una interfaz con un nivel de seguridad menor, no requiere una lista de acceso
- Trafico de una interfaz menor a una mayor deberá ser permitido por una lista de acceso
- Tráfico de una interfaz con el mismo nivel de seguridad debe tener alguno de los siguientes comandos:
 - same-security-traffic permit intra-interface**
 - same-security-traffic permit inter-interface**

Configuración de las listas de acceso

- Simplemente se crea la lista de acceso y al final solo queda aplicar esta a una interfaz.

- Ejemplo:

```
access-list Out_in permit ip any host 192.168.12.100  
access-group Out_in in interface outside
```

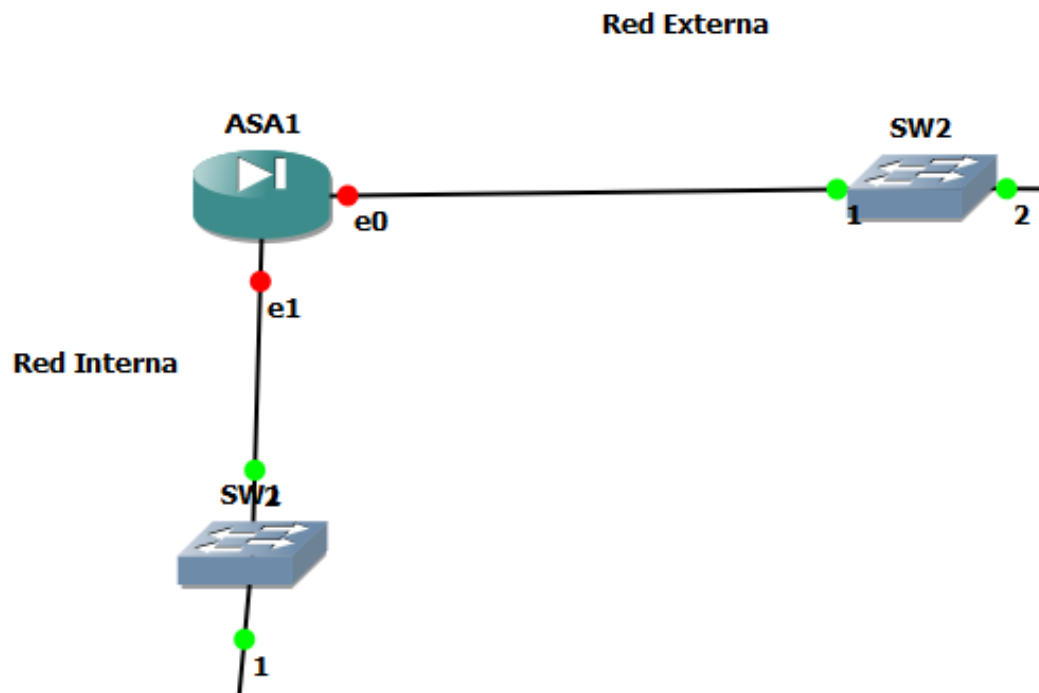


Configuración de las listas de acceso

- Recalcar la dirección en la cual se aplica la lista de acceso.

Tráfico que va a entrar al ASA :In

Tráfico que va a salir del ASA :Out



Verificación de las Listas de Acceso

- -Show access-list

```
access-list inserve80 line 1 extended permit tcp any host 10.10.33.10 eq www  
(hitcnt=1) 0x2586e119
```

```
access-list inserve80 line 2 extended permit tcp any host 10.10.33.10 eq ftp  
(hitcnt=100) 0x6e931665
```

- Show ip access-group

```
access-group outside_in in interface outside
```

Configurando Nat y ACL

- En el siguiente laboratorio llevaremos a cabo la configuración de los diferentes tipos de NAT en 8.3
- De igual manera realizaremos la configuración de las listas de acceso.
- Comprobaremos la configuración mediante el uso de la herramienta de “Packet-tracer” ; la cual nos permitirá verificar todas las políticas que el ASA utiliza en el flujo de tráfico.

Pregunta a la audiencia número 3

¿Conoce usted el monitoreo de rutas por SLA?

- a) Me gustaría conocer acerca de SLA.
- b) Tengo conocimiento teórico pero no lo he utilizado.
- c) Lo he utilizado algunas veces
- d) Sé perfectamente cómo funciona

Monitoreo de rutas por SLA



¿Qué es SLA?

- Funcionalidad que nos permitirá determinar si una ruta está disponible o no.
 - Si la ruta está disponible todo va a transcurrir normal.
 - Si la ruta no lo está, el proceso de SLA buscará una ruta alterna.
- Disponible a partir de 7.2(1)
- No permite la distribución de carga o Enrutamiento basado en origen (PBR).
- Recalcar que la única forma de que una ruta estática se remueva de la tabla de enrutamiento es si la interfaz asociada a esa ruta falla.

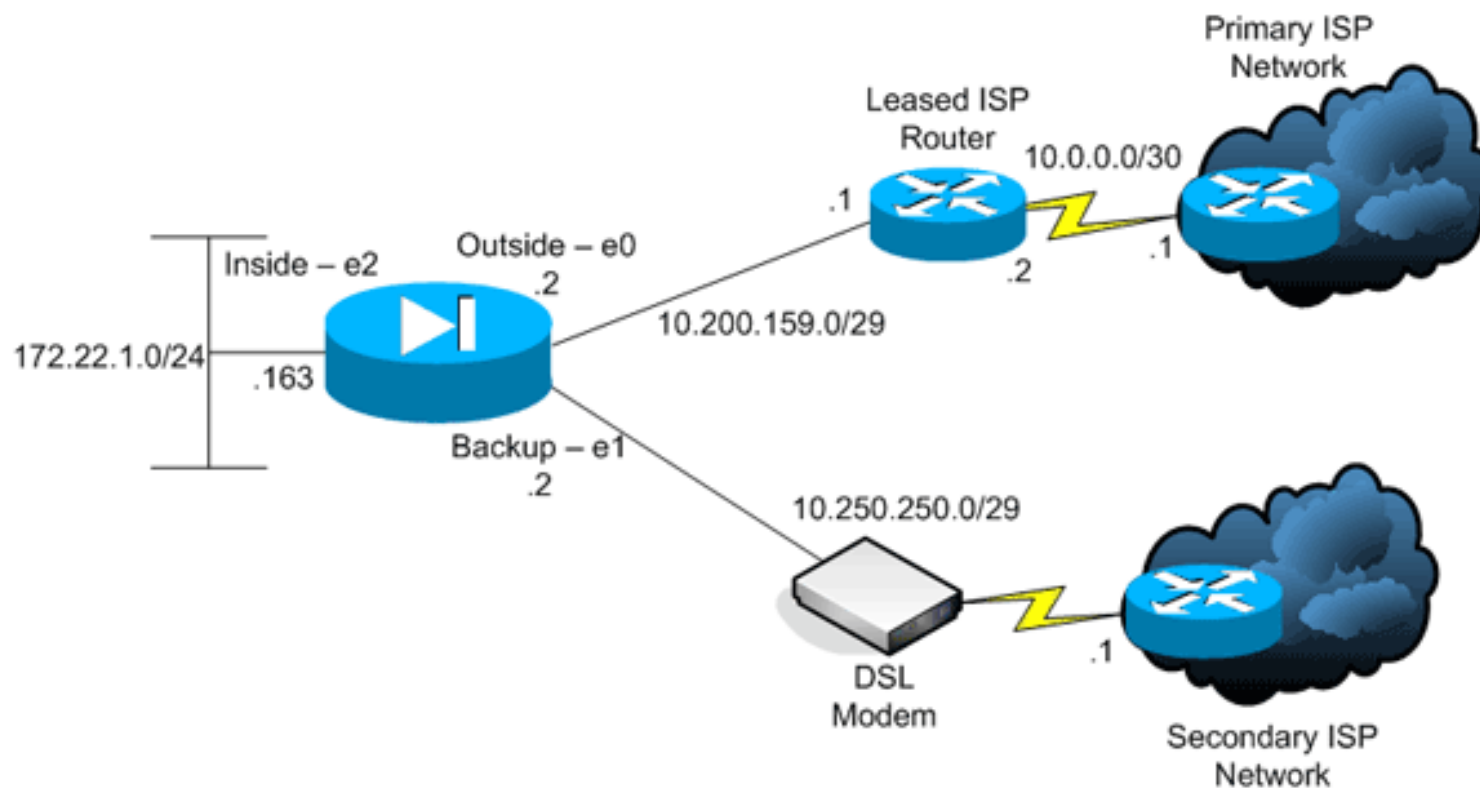
¿Cómo funciona SLA?

- Funciona mediante el monitoreo de un objeto a través de una ruta específica
- El monitoreo consiste en configurar un objeto y enviarle pruebas (Paquetes de ICMP tipo 8) y esperar que éste responda (Paquetes ICMP tipo 0) , si no responde en el lapso de tiempo configurado se determina que la ruta fallo.
- Si el objeto no responde a estas pruebas inmediatamente se utilizará una ruta previamente configurada como alterna, de igual manera se seguirán enviando pruebas por la ruta primaria, cuando el objeto empieza a responder la ruta primaria será tomada en cuenta de nuevo.

¿Dónde esperamos ver SLA?

- SLA se espera utilizar en situaciones en las cuales una sola ruta hacia un destino no es suficiente, ya que se quiere proveer redundancia en caso de que la ruta principal falle.
- Por ende se va a ver en situaciones como las siguientes:
La mas común va a ser para el uso de dos ISP's o simplemente para tener una ruta alterna a un destino específico.

Monitoreo de SLA



Configuración de SLA

- Partiremos del punto que ya existen dos interfaces conectadas hacia internet con su respectiva configuración de NAT.

interface GigabitEthernet0/0	interface GigabitEthernet0/2
<pre>nameif primario security-level 0 ip address 10.198.28.1 255.255.255.0 Nat (inside,primario) source dynamic any interface</pre>	<pre>nameif secundario security-level 0 ip address 10.10.10.1 255.255.255.0 Nat (inside,secundario) source dynamic any interface</pre>

Configuración de SLA

- Ahora crearemos las rutas respectivas en el ASA, recordando que en el ASA sólo puede existir una ruta hacia un destino, por ende sólo puede haber una ruta por defecto (Será tomada la del menor costo de métrica)

```
SLA-Lab(config)# route primario 0 0 10.198.28.2 1
```

```
SLA-Lab(config)# route secundario 0 0 10.1.1.2 254
```

Configuración de SLA

- Resultado del comando Show route

Gateway of last resort is 10.198.28.2 to network 0.0.0.0

```
C    192.168.215.0 255.255.255.0 is directly connected, inside
C    10.10.10.0 255.255.255.0 is directly connected, secundario
C    10.198.28.0 255.255.255.0 is directly connected, primario
S*   0.0.0.0 0.0.0.0 [1/0] via 10.198.28.2, primario
```

Como podemos observar solo se introduce una ruta en la tabla de enrutamiento, la que tenga menor métrica.

Configuración de SLA

- A continuación pasaremos a configurar el proceso de SLA

```
SLA-Lab(config)# sla monitor 123
```

```
SLA-Lab(config)# type echo protocol ipicmpEcho 4.2.2.2 interface primario
```

```
SLA-Lab(config-sla-monitor-echo)# num-packets 3
```

```
SLA-Lab(config-sla-monitor-echo)# frequency 10
```

```
SLA-Lab(config)# sla monitor schedule 17 life forever start-time now
```



Configuración de SLA

- Por último asociaremos el proceso de SLA con una ruta estática

```
SLA-Lab(config)# track 8 rtr 123 reachability
```

```
SLA-Lab(config)#Show run route | include track  
route primario 0.0.0.0 0.0.0.0 10.198.28.1 1 track 8
```

Como observamos el ASA dinámicamente le asigna a la ruta con la métrica mas baja el proceso de SLA.

Palabras Clave en SLA

- ***Number of packets:*** Número de paquetes ICMP a monitorear.
- ***Frequency:*** Cada cuanto se envían los paquetes ICMP.
- ***Timeout:*** Después de cuando se considera que la respuesta no fue recibida.
- ***Threshold:*** Determina luego de cuanto tiempo, se realiza una infracción al proceso de SLA (se espera una respuesta)

Verificación de SLA

```
pix# show sla monitor operational-state
Entry number: 123
Modification time: 13:59:37.825 UTC Thu Oct 12 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 385
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 15:03:27.825 UTC Thu Oct 12 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0          RTTMin: 0          RTTMax: 0
NumOfRTT: 0        RTTSum: 0          RTTSum2: 0
```


Verificación de SLA

```
pix# show sla monitor configuration 123
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.0.0.1
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 10
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

Debug SLA

- **debug sla monitor trace**

Si el objeto responde a las pruebas:

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: RTT=3 OK
IP SLA Monitor(123) echo operation: RTT=3 OK
IP SLA Monitor(123) echo operation: RTT=4 OK
IP SLA Monitor(123) Scheduler: Updating result
```

Si el objeto no responde a las pruebas:

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) Scheduler: Updating result
```

Problemas más comunes con SLA

- Se deniega el tráfico ICMP en la interfaz donde se espera monitorear el objeto.
- El dispositivo a monitorear no acepta paquetes ICMP o no se puede acceder mediante la interfaz asociada.
- Dudas con respecto a si el uso del ASA como dispositivo de VPN se ve afectado con la configuración de SLA.

Referencias

- Referencia 1

<https://supportforums.cisco.com/docs/DOC-12690>

-

Referencia 2

http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/nat_objects.html

- Páginas de Soporte:

- <http://www.cisco.com/en/US/docs/security/asa/asa83/upgrading/migrating.html>

- <http://www.cisco.com/en/US/docs/security/asa/asa83/release/notes/asarn83.html>

- http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00806e880b.shtml

Más referencias

- ASA 8.3 Upgrade - What You Need to Know

<https://supportforums.cisco.com/docs/DOC-12690>

- ASA NAT Migration problems when upgrading to 8.3; Syslog "%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows"

<https://supportforums.cisco.com/docs/DOC-12569>

- ASA 8.3 Upgrade - What You Need to Know

<https://supportforums.cisco.com/videos/2200>

- VIDEO: Cisco ASA version 8.3 and 8.4 NAT Configuration Example

<https://supportforums.cisco.com/docs/DOC-12324>

¡ Ahora puede realizar sus preguntas al panel de expertos!

Use el panel de preguntas y respuestas (Q&A) para preguntar a los expertos ahora. Ellos empezarán a responder.



Sesión de Preguntas y Respuestas

El experto responderá verbalmente algunas de las preguntas que hayan realizado. Use el panel de preguntas y respuestas (Q&A) para preguntar a los expertos ahora



Nos interesa su opinión!!!

Habr  un sorteo con los que llenen las preguntas de evaluaci n.

Tres asistentes recibir n un

Regalo sorpresa

Para llenar la evaluaci n haga click en el link que est  en el chat. Tambi n saldr  autom ticamente al cerrar el browser de la sesi n.

Pregunte al Experto

Si tiene preguntas adicionales pregunte aquí

<https://supportforums.cisco.com/thread/2169082>

Julio responderá del 4 de septiembre al 14 de septiembre del 2012.



Próximo Webcast en español

Tema: Configuración y Resolución de Problemas del Protocolo H323.

Martes 16 de octubre del 2012

9:00 a.m. Ciudad de México

9:30 a.m. Caracas

11:00 a.m. Buenos Aires

4:00 p.m. Madrid

Con **Pablo González** del TAC
Latinoamerica



Durante esta sesión en vivo usted podrá realizar todas sus preguntas acerca del tema.

Próximo Pregunta al Experto

Tema: Cisco TelePresence Video Communication Server (VCS): Configuración e Integración con CUCM y Lync 2010.

Con el Experto: Jesús Valdéz

Aprenda y haga todas sus preguntas acerca del tema.

El evento estará disponible del lunes 17 de septiembre al viernes 28 de septiembre



Próximo Webcast en inglés

Tema: Cable Modem Termination Systems (CMTS): Architecture, Configuration, and Troubleshooting



Miércoles 12 de septiembre

10.00 a.m. Ciudad de México

10:30 a.m. Caracas

12:00 p.m. Buenos Aires

4:00 p.m. Madrid

Con el experto:

Eric Bautista

Durante este evento en vivo usted tendrá un panorama de los Sistemas de Terminación de Cable Modem y conocerá las configuraciones más comunes y cómo resolver los problemas que más se presentan.

Registration for this live Webcast at

<http://goo.gl/43qTw>

Webcast en inglés de octubre

Tema: Troubleshooting SSL VPN on ASA



Martes 30 de octubre

9:00 a.m. Ciudad de México

10:30 a.m. Caracas

12.00 p.m. Buenos Aires

4:00 p.m. Madrid

Con el experto de Cisco:

Jazib Frahim

Durante este evento en vivo adquirirá conocimientos de cómo solucionar problemas de Secure Socket Layer- (SSL-) con SSL VPN en Cisco ASA's.

Registration for this live Webcast opens at the beginning of September @

<https://supportforums.cisco.com/community/netpro/expert-corner#view=webcasts>

Pregunta el Experto-inglés



Tema: RF Gateway 1 (RFGW 1) - Installation, Operation, and Troubleshooting

Con el experto de Cisco: **Ron Hanson**

Haga preguntas acerca de la configuración, operación y resolución de problemas del RF Gateway 1



Tema: Intrusion Prevention System (IPS)

Con el experto de Cisco: **Robert Albach**

Haga preguntas acerca de la configuración y resolución de problemas del IPS.

Ambos eventos terminan el viernes 7 de septiembre



Tema: Concepts, Configuration and Troubleshooting Layer 2 MPLS VPN – Any Transport over MPLS (AToM)

Con el experto de Cisco: **Vignesh R. P.**

Pregunte y aprenda acerca de los conceptos, configuración y resolución de problemas de la capa 2 MPLS VPN-cualquier transporte sobre MPLS (AToM)

Evento disponible del 10 de septiembre al 21 de septiembre

<https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts>

Facebook Forum en inglés

Tema: Migration Best Practices for ASA 8.3/8.4



Jueves 6 de septiembre

11:00 a.m. Ciudad de México

11:30 a.m. Caracas

1:00 p.m. Buenos Aires

6:00 p.m. Madrid

Con el experto de Cisco:

Praveena Shanubhogue

Aprenda acerca de mejores prácticas que se deben tener mientras se migra de la versión 8.2, o previas, a 8.3, o posteriores. Además, podrá preguntar acerca de las nuevas características y conocer los bugs o problemas conocidos que deben ser tomados en cuenta durante la migración.

RSVP @

<http://www.facebook.com/CiscoSupportCommunity>

Lo invitamos a colaborar activamente en CSC en español y en nuestras redes sociales

<https://supportforums.cisco.com/community/spanish>
<https://supportforms.cisco.com>



Español: <http://www.facebook.com/CiscoLatinoamerica>
Inglés: <http://www.facebook.com/CiscoSupportCommunity>



Español: <http://www.facebook.com/CiscoLatinoamerica>
Inglés: http://twitter.com/#!/cisco_support



Español: <http://www.youtube.com/user/CiscoLatam>
Inglés: <http://www.youtube.com/user/ciscosupportchannel>



Inglés: <http://itunes.apple.com/us/app/cisco-technical-support/id398104252?mt=8>



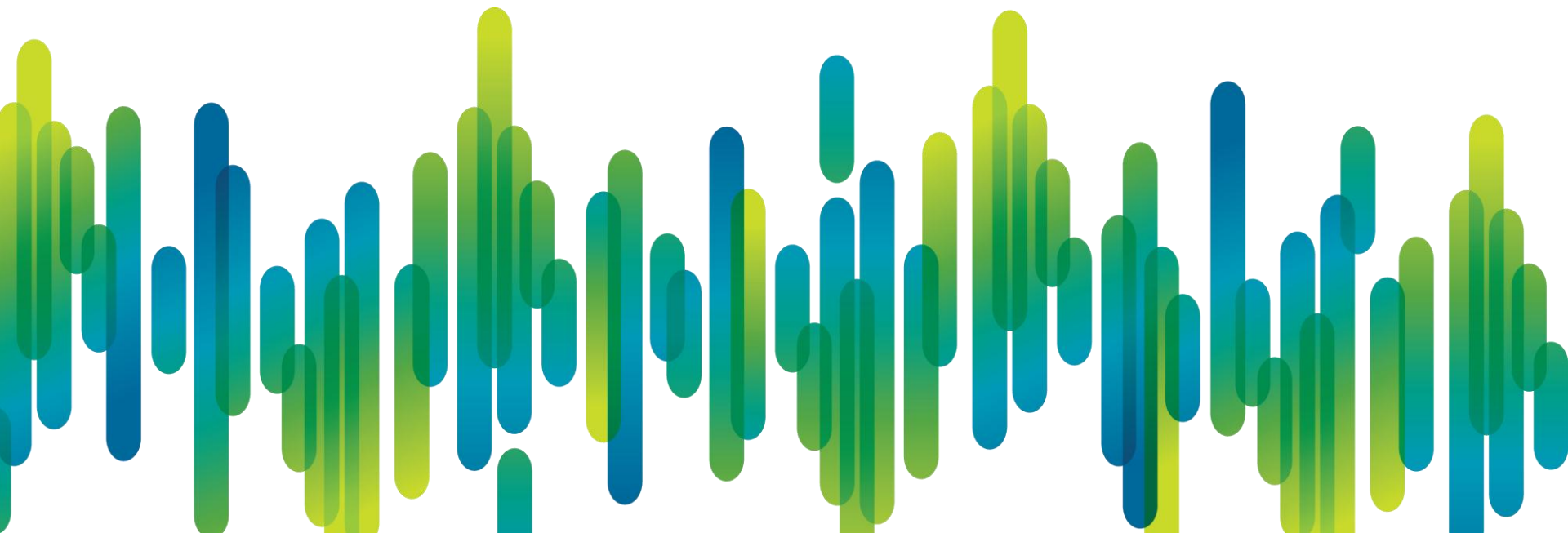
Inglés: <http://www.linkedin.com/groups/CSC-Cisco-Support-Community-3210019>



<https://plus.google.com/110418616513822966153?prsrc=3#110418616513822966153/posts>

Muchas gracias
por su asistencia

Por favor complete la encuesta de evaluación de
este evento y gane premios



Thank you.

