# Ejemplo de Configuración de ASA 8.4(x) Conecta una Sola Red Interna a Internet

## Contenido



## Introducción

Este documento describe cómo configurar Cisco Adaptive Security Appliance (ASA) con la versión 8.4(1) para su uso con una única red interna.

Consulte PIX/ASA: Ejemplo de Conexión de una Red Interna Única con Configuración de Internet para la misma configuración en el ASA con las Versiones 8.2 y anteriores.

## Prerequisites

### Requirements

No hay requisitos previos específicos para este documento.

### Componentes Utilizados

La información en este documento se basa en ASA con la versión 8.4(1).

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

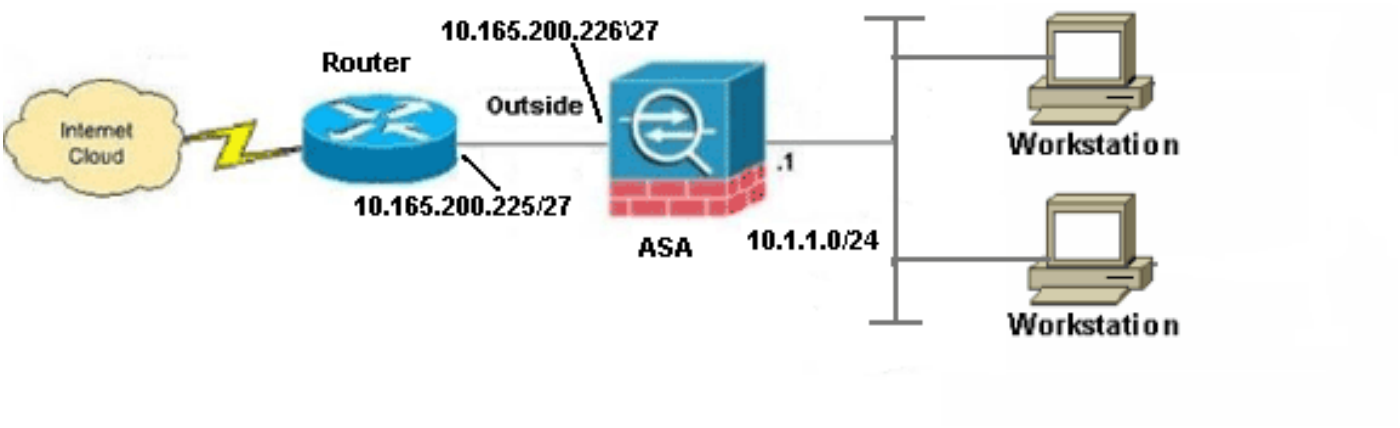
# Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

> **Nota:** Para encontrar la información adicional en los comandos usados en este documento, use la Command Lookup Tool (clientes registrados solamente).

## Diagrama de la red

En este documento, se utiliza esta configuración de red:




> **Nota:** Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918, que se han utilizado en un entorno de laboratorio.

## Configuración de ASA 8.4

En este documento, se utilizan estas configuraciones:

- Configuración del router
- Configuración de ASA 8.4 y posteriores

### Configuración del router

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R3640_out
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/1
ip address 10.165.200.225 255.255.255.224
no ip directed-broadcast

!
ip classless
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

## Configuración de ASA 8.4 y posteriores

```
ASA#show run
: Saved
:
ASA Version 8.4(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- Configure the outside interface.

!
interface GigabitEthernet0/0
```

```
nameif outside
security-level 0
ip address 10.165.200.226 255.255.255.224

!--- Configure the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
boot system disk0:/asa841-k8.bin

ftp mode passive
!
!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- NAT rule will Port Address Translate (PAT) to the outside interface IP
!--- on the ASA (or 10.165.200.226) for Internet bound traffic.
!
object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
!
nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface
!
route outside 0.0.0.0 0.0.0.0 10.165.200.225
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
```

```
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

**Nota:** Para obtener más información sobre la configuración de la traducción de direcciones de red (NAT) y la traducción de direcciones de puerto (PAT) en ASA versión 8.4, consulte Información sobre NAT.

Para obtener más información sobre la configuración de las listas de acceso en ASA versión 8.4, refiérase a Información sobre Listas de Acceso.

# Verificación

Intente acceder a un sitio web a través de HTTP con un navegador web. Este ejemplo utiliza un sitio alojado en 198.51.100.100. Si la conexión se realiza correctamente, este resultado se puede ver en ASA CLI:

## Conexión

```
ASA(config)# show connection address 10.1.1.154
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, idle 0:00:06, bytes 937,
flags UIO
```

El ASA es un firewall con información de estado y se permite el retorno del tráfico desde el servidor web a través del firewall porque coincide con una ***conexión*** en la tabla de conexión del

firewall. El tráfico que coincide con una conexión que existe previamente se permite a través del firewall sin ser bloqueado por una ACL de interfaz.

En la salida anterior, el cliente de la interfaz interna estableció una conexión con el host 198.51.100.100 fuera de la interfaz externa. Esta conexión se realiza con el protocolo TCP y ha estado inactiva durante seis segundos. Los indicadores de conexión indican el estado actual de esta conexión. Puede encontrar más información sobre los indicadores de conexión en Indicadores de conexión TCP de ASA.

## Syslog

```
ASA(config)# show log | in 10.1.1.154

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.1.1.154/58799 to outside:10.165.200.226/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.1.1.154/58799 (10.165.200.226/58799)
```

El firewall de ASA genera syslogs durante el funcionamiento normal. El nivel de detalle de los syslogs depende de la configuración de registro. El resultado muestra dos syslogs que se ven en el nivel seis, o nivel **'informativo'**.

En este ejemplo, se generan dos syslogs. El primero es un mensaje de registro que indica que el firewall ha creado una **traducción**, específicamente una traducción TCP dinámica (PAT). Indica la dirección IP de origen y el puerto y la dirección IP traducida a medida que el tráfico atraviesa desde el interior a las interfaces externas.

El segundo syslog indica que el firewall ha creado una conexión en su tabla de conexiones para este tráfico específico entre el cliente y el servidor. Si el firewall se configuró para bloquear este intento de conexión, o algún otro factor inhibió la creación de esta conexión (restricciones de recursos o una posible configuración incorrecta), el firewall no generaría un registro que indique que la conexión se creó. En su lugar, registraría una razón para que se negara la conexión o una indicación sobre qué factor impedía que se creara la conexión.

## Traducciones NAT (Xlate)

```
ASA(config)# show xlate local 10.1.1.154
3 in use, 80 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle
0:02:42 timeout 0:00:30
```

Como parte de esta configuración, PAT se configura para traducir las direcciones IP del host interno a las direcciones que son enrutables en Internet. Para confirmar que se crean estas traducciones, puede verificar la tabla xlate (translation). El comando **show xlate,** cuando se combina con la palabra clave **local** y la dirección IP del host interno, muestra todas las entradas presentes en la tabla de traducción para ese host. La salida anterior muestra que hay una traducción actualmente construida para este host entre las interfaces interna y externa. La IP y el puerto del host interno se traducen a la dirección 10.165.200.226 por nuestra configuración. Los indicadores enumerados, r i , indican que la traducción es **dinámica** y un **portmap**. Puede

encontrar más información sobre las diferentes configuraciones de NAT aquí: Información sobre NAT.

# Troubleshoot

ASA proporciona varias herramientas con las que resolver problemas de conectividad. Si el problema persiste después de verificar la configuración y verificar el resultado mencionado anteriormente, estas herramientas y técnicas pueden ayudar a determinar la causa de su falla de conectividad.

## Packet-Tracer

```
ASA(config)# packet-tracer input inside tcp 10.1.1.154 1234 198.51.100.100 80


--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

La funcionalidad **packet tracer** en el ASA le permite especificar un *paquete simulado* y ver todos los pasos, verificaciones y funciones que el firewall realiza cuando procesa el tráfico. Con esta herramienta, es útil identificar un ejemplo de tráfico que cree que *debería* permitirse pasar a través del firewall, y usar ese 5-tupple para simular tráfico. En el ejemplo anterior, se utiliza el rastreador de paquetes para simular un intento de conexión que cumpla con estos criterios:

- El paquete simulado llega al **interior**.
- El protocolo utilizado es **TCP**.
- La dirección IP del cliente simulado es 10.1.1.154.
- El cliente envía el tráfico originado en el puerto **1234**.
- El tráfico se destina a un servidor en la dirección IP 198.51.100.100.
- El tráfico está destinado al puerto 80.

Observe que no hubo mención de la interfaz **externa** en el comando. Esto es por diseño de Packet Tracer. La herramienta le indica cómo el firewall procesa ese tipo de intento de conexión, lo que incluye cómo lo enrutaría y desde qué interfaz. Se puede encontrar más información sobre el rastreador de paquetes en Seguimiento de paquetes con Packet Tracer.

## Captura

```
ASA# capture capin interface inside match tcp host 10.1.1.154 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#   show capture capin
```

```
3 packets captured

  1: 11:31:23.432655       10.1.1.154.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712518       198.51.100.100.80 > 10.1.1.154.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.1.1.154.58799 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       10.165.200.226.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712472       198.51.100.100.80 > 10.165.200.226.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       10.165.200.226.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

El firewall ASA puede capturar el tráfico que entra o sale de sus interfaces. Esta funcionalidad de captura es fantástica porque puede demostrar definitivamente si el tráfico llega a un firewall o sale de él. El ejemplo anterior mostró la configuración de dos capturas denominadas **capin** y **capout** en las interfaces interna y externa respectivamente. Los comandos capture utilizaron la palabra clave **match**, que le permite ser específico sobre qué tráfico desea capturar.

Para la **capa de** captura**,** indicó que deseaba hacer coincidir el tráfico visto en la interfaz interna (entrada o salida) que coincide con el **host tcp 10.1.1.154 host 198.51.100.100**. En otras palabras, desea capturar cualquier tráfico TCP que se envíe desde el **host 10.1.1.154** al **host 198.51.100.100** o **viceversa**. El uso de la palabra clave match permite que el firewall capture ese tráfico bidireccionalmente. El comando capture definido para la interfaz exterior no hace referencia a la dirección IP interna del cliente porque el firewall realiza PAT en esa dirección IP del cliente. Como resultado, no puede coincidir con esa dirección IP de cliente. En cambio, este ejemplo usa **any para indicar que todas las direcciones IP posibles coincidirían con esa condición.**

Después de configurar las capturas, intentaría establecer una conexión de nuevo y procedería a ver las capturas con el comando **show capture *<capture_name>***. En este ejemplo, puede ver que el cliente pudo conectarse con el servidor como se ve en el intercambio de señales TCP de 3 vías visto en las capturas.

# Información Relacionada

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems