



Webcast com Especialistas em Tecnologia da Comunidade Cisco:

Soluções de Problema em Cisco Adaptive Security Appliances (ASA)

Davi Garcia
Especialista em Segurança

28 de Agosto de 2012

Webcast com Especialistas em Tecnologia da Comunidade Cisco

- O especialista de hoje é o Engenheiro de Suporte à Clientes da Cisco do Brasil **Davi Garcia (davigar)**.
- Poderá perguntar questões sobre técnicas e/ou ferramentas básicas para Soluções de Problema na plataforma Cisco ASA.



Davi Garcia

Engenheiro de Suporte a Clientes

Obrigado por estar conosco hoje

- A apresentação incluirá algumas perguntas para o público.
- Convidamos você a participar ativamente das perguntas que faremos durante a sessão



Obrigado por estar conosco hoje

- Se desejar baixar uma cópia da apresentação de hoje, vá ao endereço indicado no chat ou use este link:

<https://supportforums.cisco.com/community/portuguese/canto-dos-especialistas/webcasts>



Primeira Pergunta

Qual seu nível de experiência com o ASA?

- a) Ouvi falar anteriormente sobre a plataforma.**
- b) Tive oportunidade de trabalhar em ambientes com ASA.**
- c) Estou estudando para implementar em produção.**
- d) Tenho ASA em meu ambiente de produção.**

Faça suas perguntas agora!

Use o painel de perguntas e respostas (Q&A) para perguntar ao especialista agora. Ele começará a responder.





Webcast com Especialistas em Tecnologia da Comunidade Cisco:

Soluções de Problema em Cisco Adaptive Security Appliances (ASA)

Davi Garcia

Especialista em Segurança

28 de Agosto

Agenda

- **Introdução:**

- Portfólio do Cisco ASA.
- Funcionamento básico.
- Metodologia de Troubleshooting.

- **Ferramentas:**

- Syslog.
- Filtrando Saídas de Comandos na CLI.
- Tabela de Conexões (“show conn”).
- Captura de Pacotes (“capture”).
- Simulador de Pacotes (“packet-tracer”).

- **Dúvidas.**

Introdução



Introdução

Portfólio Cisco ASA

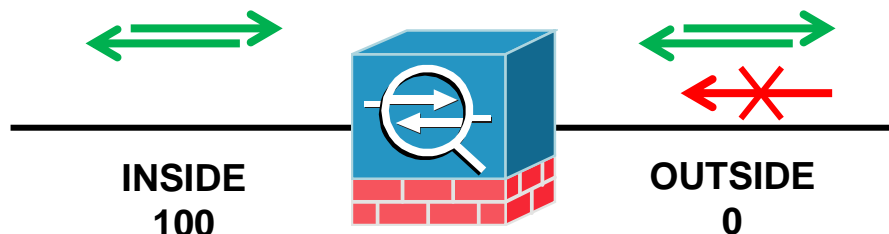


- A linha de produtos **Cisco Adaptive Security Appliances (ASA) 5500** foi introduzida em 2005, consolidando funcionalidades de Firewall, VPN, IPS e filtro de conteúdo (Anti-X).
- Funcionalidades adicionais através do **Cisco Secure Service Module (SSM)** ou do **Cisco Security Services Card (SSC)**, para plataforma ASA 5505.
- A nova geração **5500-X** foi introduzida em 2012 e garante **maior performance** para ambientes críticos e **funcionalidade de IPS/IDS integradas em software**.

http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html

Introdução

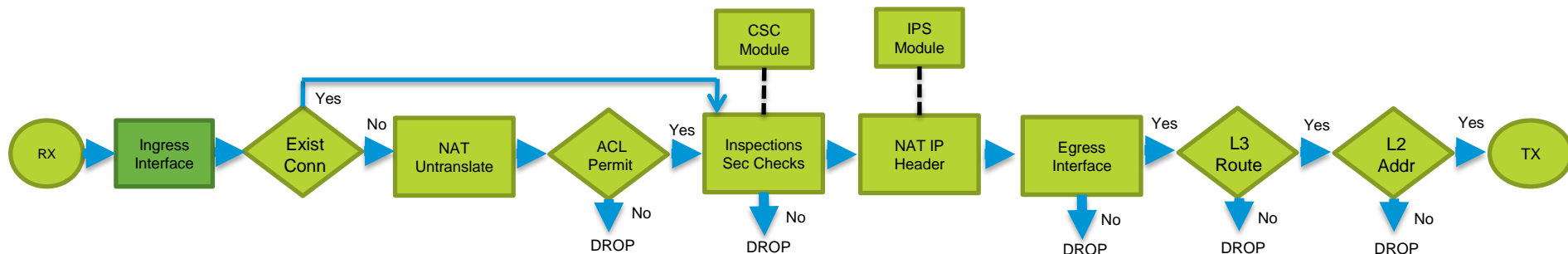
Funcionamento Básico



- O ASA é um **firewall stateful**, ou seja, mantém uma tabela interna de conexões realizadas através dele.
- Interfaces são **classificadas com nome e nível de segurança**, onde:
 - **Nível 0** significa **menor** segurança (ex.: interface de WAN)
 - **Nível 100** significa **maior** segurança (ex.: interface de LAN)
- Tráfego que flui de uma interface de **maior nível de segurança para uma menor é permitido por padrão**. O sentido oposto, **do menor nível para o maior, é proibido por padrão**.
- O **comportamento padrão pode ser alterado** por configurações de **Access Control Lists (ACL)** ou **Network Address Translation (NAT)**.

Introdução

Funcionamento Básico

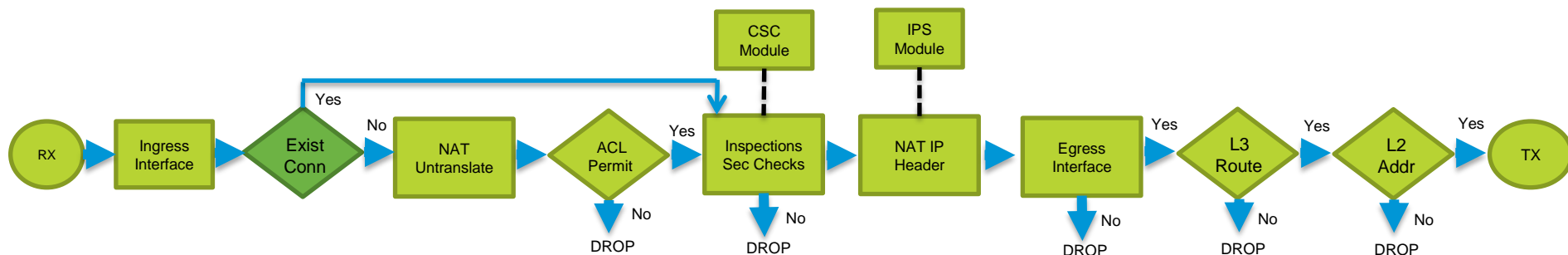


- Pacotes chegam na interface de entrada.
- Contadores de entrada são incrementados.
- Fila de entrada é um indicador de carga. Contadores de **no buffers** e **overruns** indicam descartes (possivelmente rajadas!).

```
ASA# show interface GigabitEthernet0/1
Interface GigabitEthernet0/1 "", is up, line protocol is up
  Hardware is bcm56800 rev 01, BW 1000 Mbps, DLY 10 usec
    Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
    Input flow control is unsupported, output flow control is off
    Active member of Port-channel10
    MAC address 4055.3980.0e67, MTU 1500
    IP address unassigned
    410179 packets input, 42620992 bytes, 0 no buffer
    Received 138749 broadcasts, 0 runts, 0 giants
    ...
```

Introdução

Funcionamento Básico



- Verifica se existe alguma conexão na tabela interna.
- Se existe entrada, o pacote é relacionado a uma conexão: **ignora validação de ACL.**
- Se não existe entrada:
 - Pacote TCP non-SYN, descarta e gera mensagem de log.
 - Pacote TCP SYN ou UDP, segue para a validação de ACL.

Conexão Estabelecida:

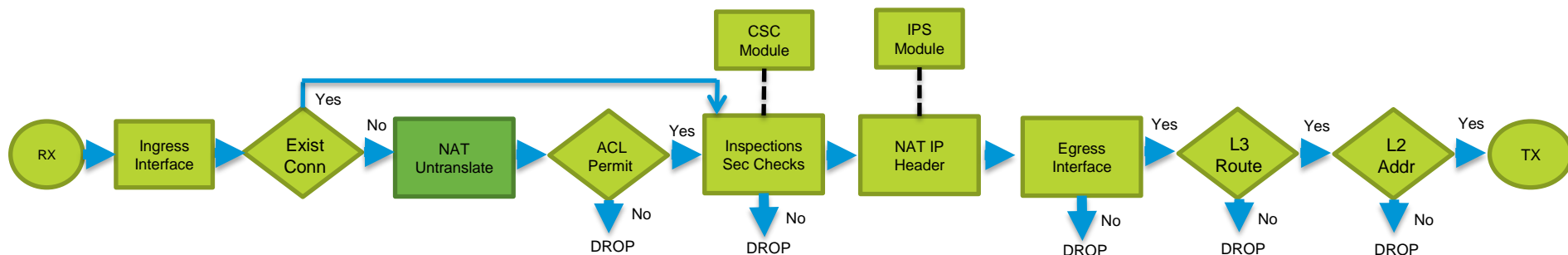
```
ASA-5540# show conn
TCP out 198.133.219.25:80 in 10.1.1.9:11030 idle 0:00:04 Bytes 1293 flags UIO
```

Mensagem de syslog quando não existe conexão e pacote TCP non-SYN:

```
ASA-6-106015: Deny TCP (no connection) from 10.1.1.9/11031 to 198.133.219.25/80 flags PSH ACK on interface inside
```

Introdução

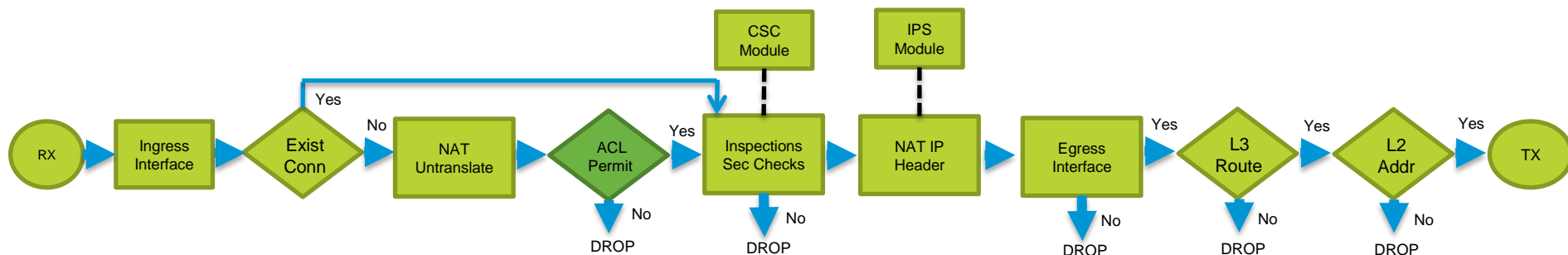
Funcionamento Básico



- Pacotes são validados e processados conforme regras de NAT. **Nesta fase é realizado o UN-NAT!**
- Na **versão 8.2 ou anterior**, pacotes são submetidos a **validação de ACL antes de sofrer UN-NAT**.
- **A partir da versão 8.3**, primeiro é feito o **UN-NAT antes da validação de ACL!**

Introdução

Funcionamento Básico



- **Primeiro pacote do fluxo é validado contra as configurações de ACL da interface de entrada.** Lembrando que as ACLs são “first match”.
- **Primeiro pacote** do fluxo confere com a ACE, incrementando o contador em 1.
- Pacotes negados são descartados e uma mensagem de log é gerada.

Pacote permitido por ACL:

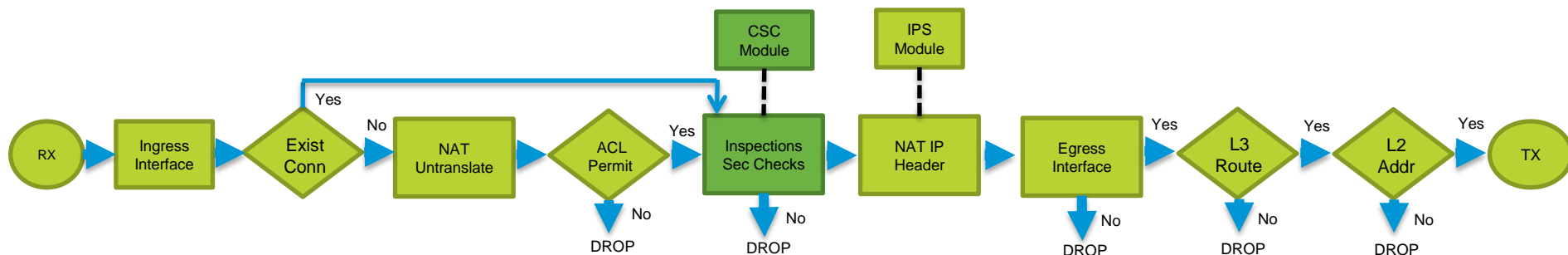
```
ASA-5540B# show access-list inside
access-list inside line 10 permit ip 10.1.1.0 255.255.255.0 any (hitcnt=1)
```

Mensagem de syslog quando pacote descartado por ACL:

```
ASA-4-106023: Deny tcp src inside:10.1.1.9/11034 dst outside:198.133.219.25/80 by access-group inside
```

Introdução

Funcionamento Básico



- Mecanismos de **inspeção são aplicadas para validar conformidade dos protocolos.**
- Inspeções customizadas (AIC - Application Inspection and Control) são realizadas, se configurado.
- **Mudança de NAT-embedded IPs no payload dos pacotes** (tráfego de voz, DNS, etc).
- **Pacotes são encaminhados para o módulo Content Security and Control (CSC), se configurado.**

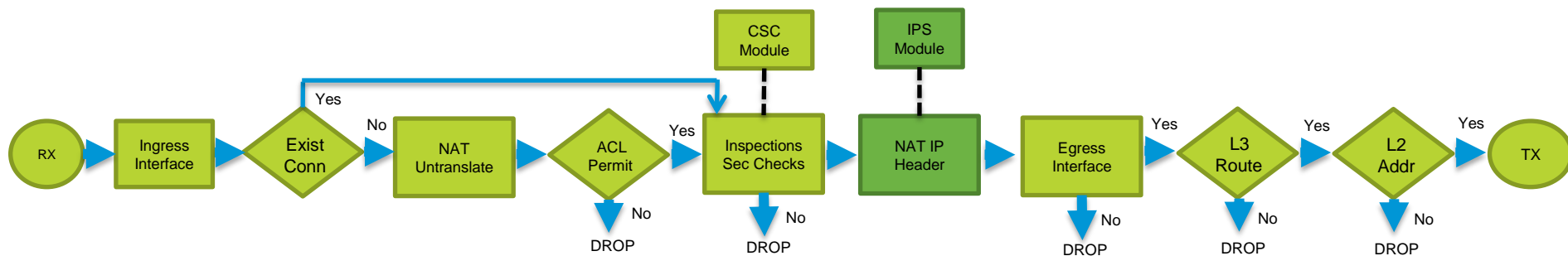
Mensagens de syslog de pacotes descartados por Validação de Segurança:

```
ASA-4-406002: FTP port command different address: 10.2.252.21(192.168.1.21) to 209.165.202.130 on interface inside
```

```
ASA-4-405104: H225 message received from outside_address / outside_port to inside_address / inside_port before SETUP
```


Introdução

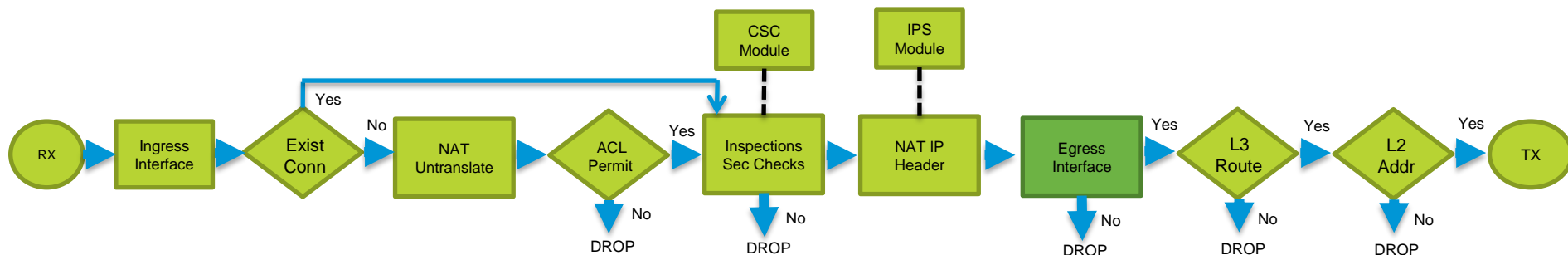
Funcionamento Básico



- Traduz os endereços da camada L3 (IP), se configurado **NAT**.
- Traduz as portas da camada L4 (TCP/UDP), se configurado **PAT**.
- Caso o pacote tenha sofrido alterações, **recalcula e atualiza os checksums!**
- **Pacotes são encaminhados para o módulo Advanced Inspection and Prevention (AIP), se configurado.**

Introdução

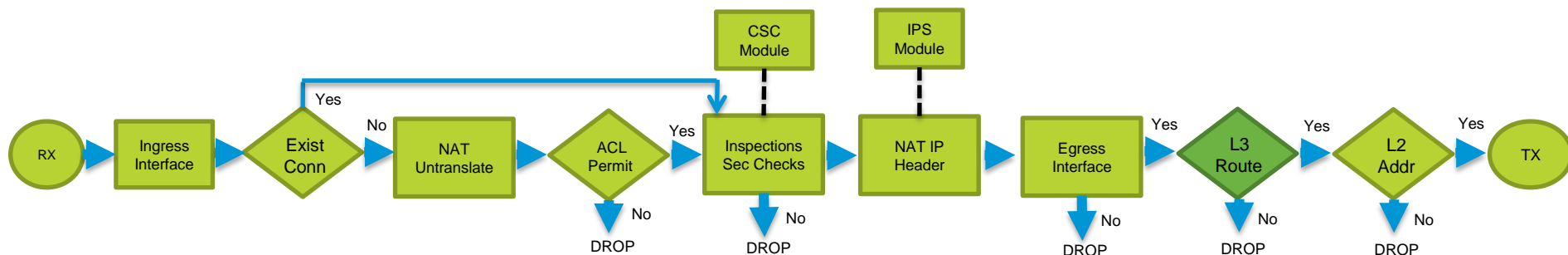
Funcionamento Básico



- O pacote é virtualmente encaminhado para a sua interface de saída (egress), mas não para o driver controlador da interface.
- A interface de saída (egress) é determinada da seguinte forma:
 - Se uma entrada na tabela de traduções (xlate) já existir para aquele tráfego, a interface de saída é determinada pela mesma e não pela tabela de roteamento.
 - Se a entrada na tabela de traduções (xlate) não existir mas o tráfego seja compatível com uma regra de NAT/PAT estática, a interface de saída é determinada pela mesma e não pela tabela de roteamento.
 - Caso nenhum dos casos anteriores ocorram, a interface de saída é determinada pela tabela de roteamento.

Introdução

Funcionamento Básico



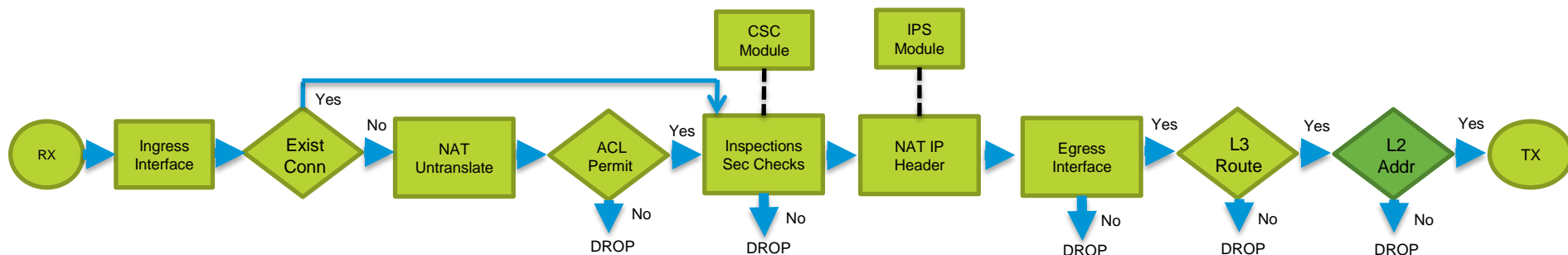
- **Uma vez definida a interface de saída, a avaliação da tabela de rotas é realizada.**
- Somente rotas que apontam para a interface de saída (egress) são consideradas válidas.
- Lembre-se: regras de NAT/PAT podem **alterar a interface de saída para uma interface diferente da que a tabela de rotas indica como válida!**

Mensagens de syslog de pacotes descartados por problemas de determinação de destino L3:

```
%ASA-6-110003: Routing failed to locate next hop for TCP from inside:192.168.103.220/59138 to dmz:172.18.124.76/23
```

Introdução

Funcionamento Básico

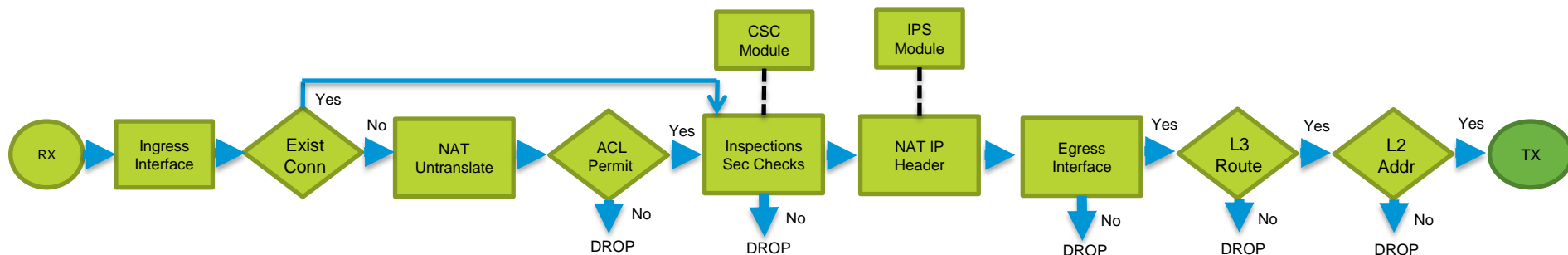


- Uma vez que a rota L3 tenha sido encontrada, e o “next-hop” determinado, **a resolução de endereço L2 (Ethernet) é executada.**
- Processo de **reescrita do cabeçalho L2** é executado.
- **Se o processo de resolução L2 falhar, nenhuma mensagem de syslog é exibida!**
Para resolver:
 - **show arp** : Não vai mostrar entrada válida para o endereço de destino.
 - **debug arp** : Irá informar que o ARP reply ainda não foi respondido.

```
arp-req: generating request for 10.1.2.33 at interface outside
arp-req: request for 10.1.2.33 still pending
```

Introdução

Funcionamento Básico



- O pacote é **transmitido fisicamente**.
- Os contadores nas interfaces são incrementados.

```
ASA# show interface GigabitEthernet 0/2
Interface GigabitEthernet0/2 "", is up, line protocol is up
  Hardware is bcm56800 rev 01, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
  Input flow control is unsupported, output flow control is off
  Active member of Port-channel11
  MAC address 4055.3980.0e68, MTU 1500
  IP address unassigned
  ...
  101315 packets output, 13086040 bytes, 0 underruns
  0 pause/resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 rate limit drops
  0 switch egress policy drops
  0 input reset drops, 0 output reset drops
```

Introdução

Metodologia de Troubleshooting

- Qualquer metodologia de solução de problemas começa com a definição do sintoma. **Quanto mais específico melhor.**
- No ponto de vista do ASA, a definição do sintoma se resume em definir com exatidão o fluxo de pacotes afetado (conexão):
 - Qual a origem da conexão afetada (endereço IP)?
 - Qual o serviço utilizado (endereço IP de destino, porta, transporte)?
 - Por qual interface o tráfego afetado deveria chegar (ingress)?
 - Por qual interface o tráfego afetado deveria sair (egress)?
 - O que está acontecendo com o tráfego afetado?
- Caso o cenário tenha funcionado anteriormente, definir:
 - O que mudou (versão de software, interface de saída, protocolo)?
 - Quando mudou?



Segunda Pergunta

Ao abrir um chamado com o TAC, quais informações adicionais são necessárias?

- a) Topologia.
- b) Saída do comando “show tech”.
- c) Topologia e Saída do comando “show tech”.
- d) Nenhuma.

Ferramentas



Ferramentas

Mensagens de syslog

- Syslog deve ser sempre o **primeiro lugar que visitamos** quando estamos resolvendo problemas.
- ASA possui um syslog bastante robusto para praticamente tudo!
- Atualmente a **versão 8.4 possui cerca de 1.913 mensagens únicas de syslog.**
- Syslogs são divididos por **nível (0-7)**
- Syslogs podem ser enviados para diversos destinos:

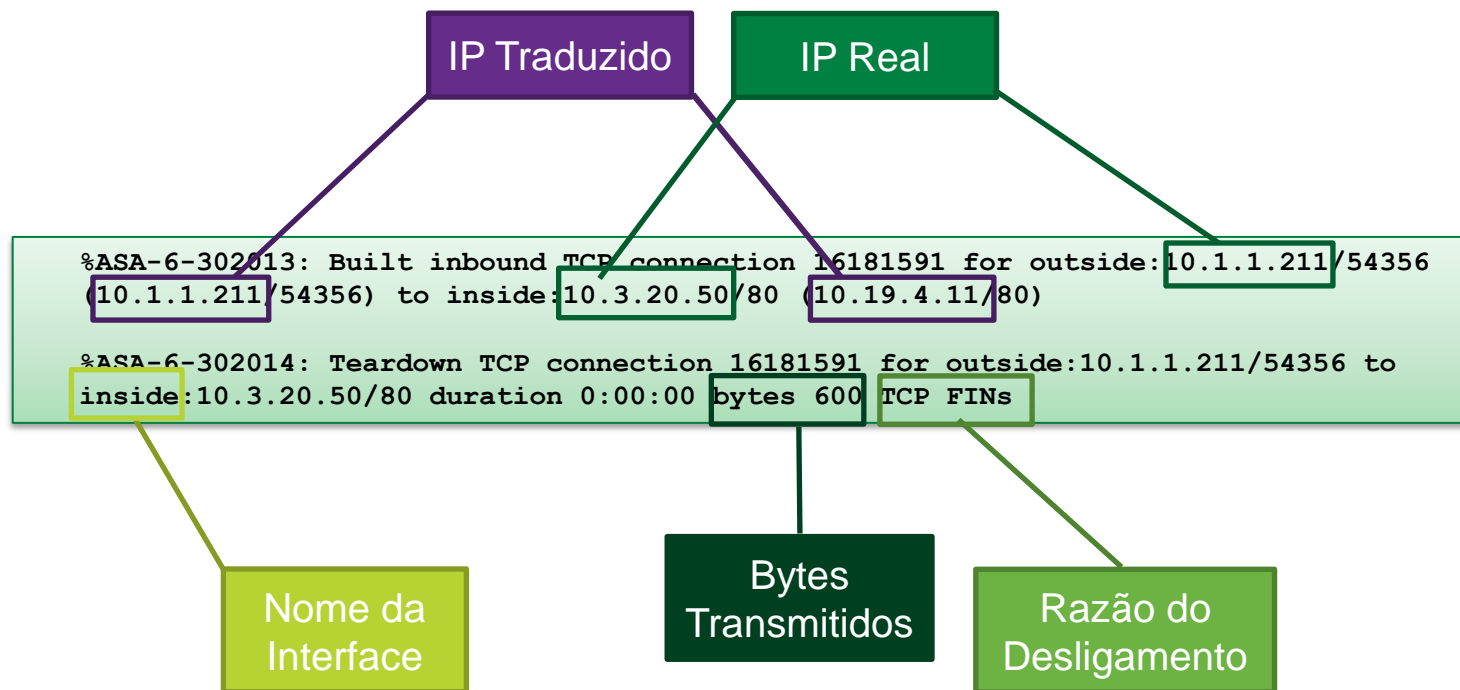
Local buffer
Terminal session
Console
Syslog server

E-mail
FTP Server
Flash (local)
SNMP server

Ferramentas

Mensagens de syslog

- Mensagens de criação/destruição de conexões são as mais úteis quando realizamos troubleshooting.



Ferramentas

Mensagens de syslog

- Quando estamos resolvendo problemas:
 - Habilitar syslog para o buffer local, geralmente no nível 7 (debugging).
 - Aumentar o tamanho default do buffer. Máximo é 1 MB (em bytes).

```
logging enable ! Habilita syslog.  
logging buffered debugging ! Configura o nível 7 para o syslog armazenado no buffer.  
!  
logging buffer-size 512000 ! Configura o tamanho do buffer para 512KB.  
logging timestamp ! Habilita timestamp nas mensagens.
```

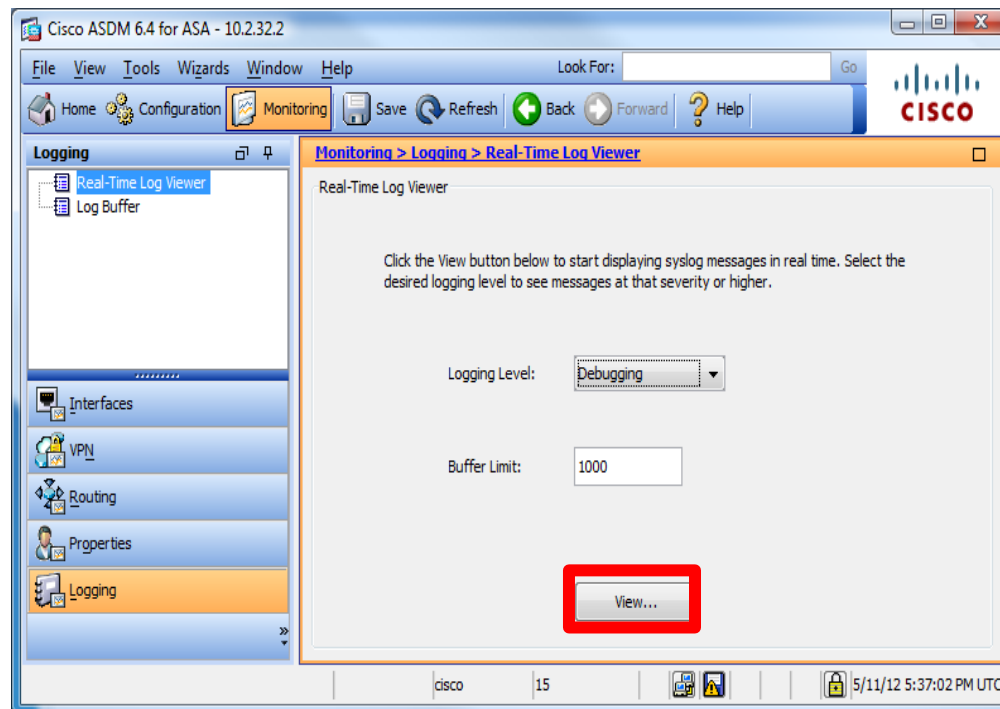
- É possível configurar para que mensagens específicas de syslog não sejam exibidas ou tenham seu nível alterado:

```
no logging message 609002 ! Desabilita a mensagem de syslog 609002.  
!  
logging message 609001 level emergencies ! Altera o nível da mensagem 609001 para 0.
```

Ferramentas

Mensagens de syslog

- Para visualizar syslog no ASDM: **Monitoring Tab → Logging**
- Especificar nível de logging do ASDM, e tamanho do buffer:



Ferramentas

Mensagens de syslog

Real-Time Log Viewer - 10.2.32.2

File Tools Window Help

Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help

Filter By: Filter Build Filter Show All Find:

Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
2	May 11 2012	17:37:50	106001	10.1.1.211	47796	209.165.32.7	80	Inbound TCP connection denied
6	May 11 2012	17:37:47	302014	10.1.1.211	39658	10.3.32.50	80	Tear down TCP connection 626
6	May 11 2012	17:37:47	302013	10.1.1.211	39658	10.3.32.50	80	Built inbound TCP connection 6
2	May 11 2012	17:37:43	106001	10.1.1.211	47732	209.165.32.7	80	Inbound TCP connection denied
6	May 11 2012	17:37:40	302014	10.1.1.211	39594	10.3.32.50	80	Tear down TCP connection 626
6	May 11 2012	17:37:40	302013	10.1.1.211	39594	10.3.32.50	80	Built inbound TCP connection 6
6	May 11 2012	17:37:38	302015	10.1.1.211	40033	10.2.32.2	161	Built inbound UDP connection 6
6	May 11 2012	17:37:38	302015	10.1.1.211	34604	10.2.32.2	161	Built inbound UDP connection 6
6	May 11 2012	17:37:38	302015	10.1.1.211	35163	10.2.32.2	161	Built inbound UDP connection 6
6	May 11 2012	17:37:38	302015	10.1.1.211	41326	10.2.32.2	161	Built inbound UDP connection 6
2	May 11 2012	17:37:36	106001	10.1.1.211	47668	209.165.32.7	80	Inbound TCP connection denied

Syslog Details

```

ASA-6-302013: Built {inbound|outbound} TCP connection_id for
interface:real-address/real-port (mapped-address/mapped-port) [(idfv_user)] to
interface:real-address/real-port (mapped-address/mapped-port) [(idfv_user)]
[(user)]

A TCP connection slot between two hosts was created.

• connection_id—A unique identifier

• interface, real-address, real-port—The actual sockets
    
```

Explanation Recommended Action Details

Emergencies Alerts Critical Errors Warnings Notifications Informational Debugging

Ferramentas

Filtrando Saídas de Comandos na CLI.

- Filtragem de saída dos comandos é importante para visualizar informações específicas ou buscar por mensagens de syslog.
- ASA suporta os seguintes filtros:
 - **include <expressão>** : Visualiza somente as linhas que contém a expressão.
 - **exclude <expressão>** : Visualiza somente as linhas que não contém a expressão
 - **grep <expressão>** : Idêntico ao “include”.
 - **grep -v <expressão>** : Idêntico ao “exclude”.
 - **begin <expressão>** : Visualiza somente linhas a partir do primeiro match.
- Exemplo:

```
! Show the syslogs minus those we aren't interested in  
ASA# show log | exclude 609001|609002|710005
```

```
! Show only TCP Built and Teardown Connections  
ASA# show log | include 302013|302014
```

Ferramentas

Filtrando Saídas de Comandos no ASDM.

Filtro no ASDM
aceita Expressões
Regulares (regex)

The screenshot shows the Real-Time Log Viewer interface. A red box highlights the filter input field containing the text "10.1.1.211". Below the filter is a table of log entries. The table has columns for Severity, Date, Time, Syslog ID, Source IP, Source Port, Destination IP, Destination Port, and Description. The log entries show various network events, including TCP connections being denied or built.

Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
6	May 11 2012	17:43:44	302014	10.1.1.211	49281	10.3.32.50	80	Tear down TCP connection 627...
6	May 11 2012	17:43:44	302013	10.1.1.211	49281	10.3.32.50	80	Built inbound TCP connection 6...
2	May 11 2012	17:43:32	106001	10.1.1.211	35539	209.165.32.7	80	Inbound TCP connection denied...
6	May 11 2012	17:43:28	302014	10.1.1.211	49217	10.3.32.50	80	Tear down TCP connection 627...
6	May 11 2012	17:43:28	302013	10.1.1.211	49217	10.3.32.50	80	Built inbound TCP connection 6...
2	May 11 2012	17:43:18	106001	10.1.1.211	35475	209.165.32.7	80	Inbound TCP connection denied...
6	May 11 2012	17:43:15	302014	10.1.1.211	49153	10.3.32.50	80	Tear down TCP connection 627...
6	May 11 2012	17:43:15	302013	10.1.1.211	49153	10.3.32.50	80	Built inbound TCP connection 6...
2	May 11 2012	17:43:11	106001	10.1.1.211	35411	209.165.32.7	80	Inbound TCP connection denied...
6	May 11 2012	17:43:10	302016	10.1.1.211	43721	10.2.32.2	161	Tear down UDP connection 626...
6	May 11 2012	17:43:10	302016	10.1.1.211	34397	10.2.32.2	161	Tear down UDP connection 626...

The Syslog Details pane shows the following text:

```
%ASA-2-106001: Inbound TCP connection denied from IP_address/port to  
IP_address/port flags tcp_flags on interface interface_name
```

An attempt was made to connect to an inside address is denied by the security policy that is defined for the specified traffic type. The IP address displayed is the real IP address instead of the IP address that appears through NAT. Possible *tcp_flags* values correspond to the flags in the TCP header that were present when the connection was denied. For example, a TCP packet arrived for which no connection state exists in the ASA, and it was dropped. The *tcp_flags* in this packet are FIN and ACK.

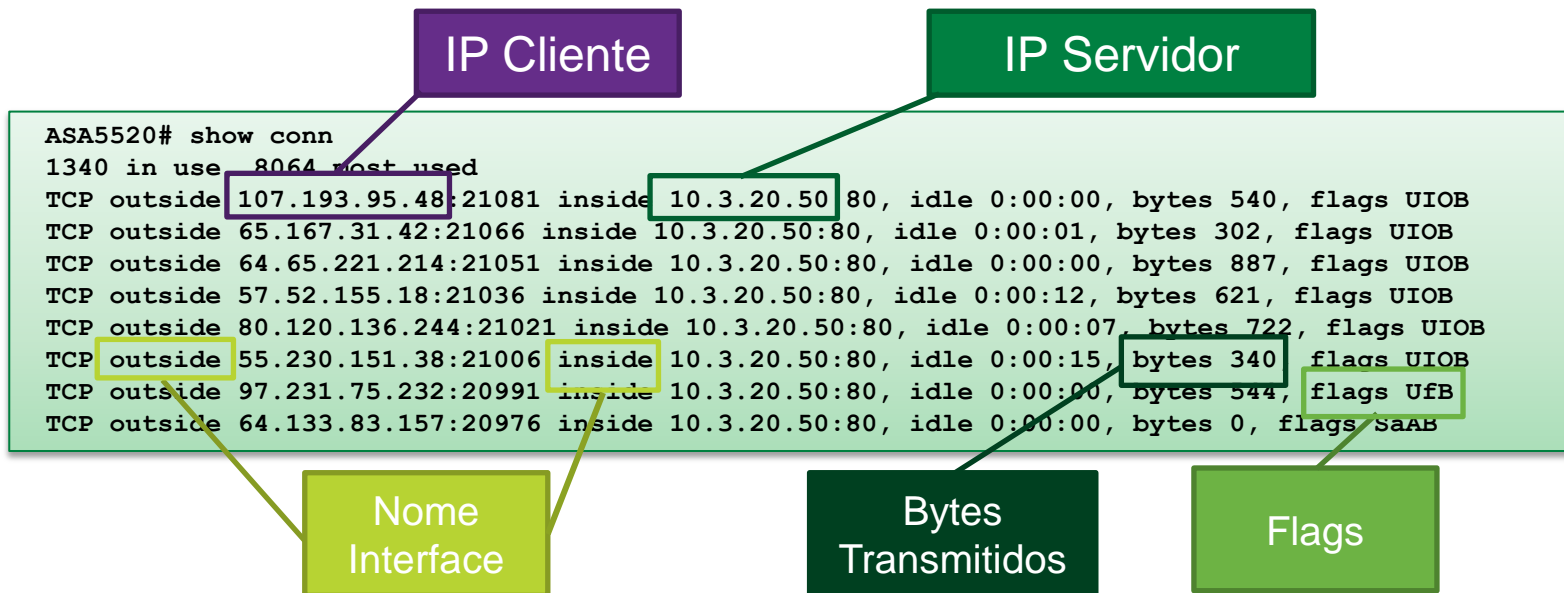
The *tcp_flags* are as follows:

- ACK—The acknowledgment number was received

Ferramentas

Tabela de Conexões

- Todo o tráfego que atravessa o ASA cria entradas na tabela de conexões.
- O comando “show conn” é utilizado para visualizar as **entradas ativas** do tabela de conexões.



Ferramentas

Tabela de Conexões

- Flags mais comuns:

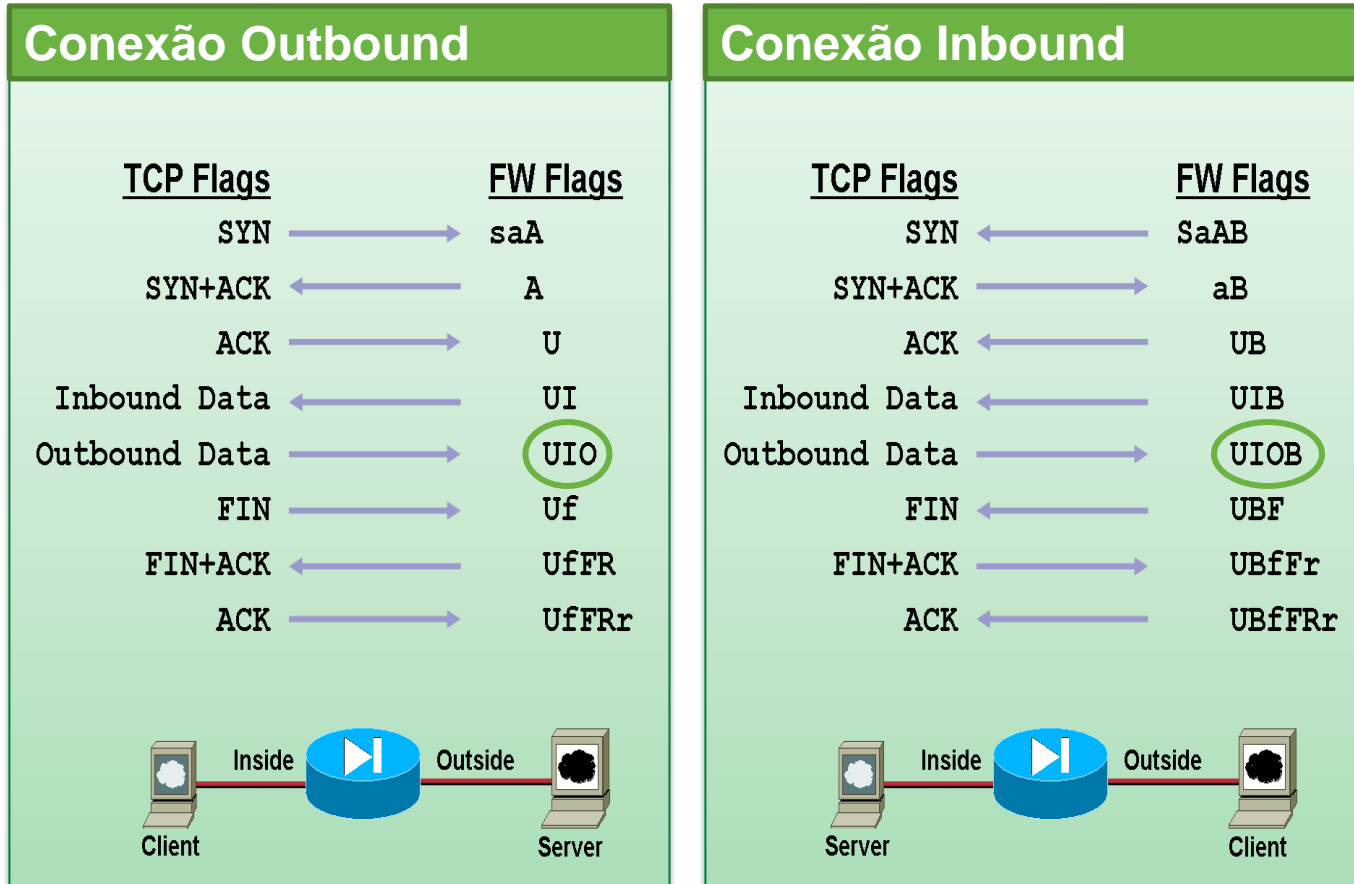
Flags
REMOVIDOS
Ao Receber
Pacotes

Flags
ADICIONADOS
Ao Receber
Pacotes

S	Awaiting Inside SYN
s	Awaiting Outside SYN
A	Awaiting Inside ACK to SYN
a	Awaiting Outside ACK to SYN
B	Initial SYN from Outside (Inbound Conn)
U	3-way Handshake Complete
I	Received Inbound Data
O	Received Outbound Data
F	Received Outside FIN
f	Received Inside FIN
R	Received Outside ACK to FIN
r	Received Inside ACK to FIN
X	Inspected by Service Module

Ferramentas

Tabela de Conexões



Ferramentas

Captura de Pacotes

- ASA provê **funcionalidades integradas de sniffer**, capaz de capturar os pacotes antes e depois dos processamentos internos.
- Por padrão, o pacote é capturado por completo. Opcionalmente podemos especificar parâmetros **packet-length**, ou **headers-only** (L2-L4).
- O critério para **limitar a captura pode ser feito por ACLs ou comando “match”**. ACLs são **unidirecionais**, enquanto o “match” é **bidirecional**.
- As capturas podem ser visualizadas na CLI/ASDM do ASA ou **exportadas no formato PCAP** (Wireshark).

<https://supportforums.cisco.com/docs/DOC-1222>

Ferramentas

Captura de Pacotes

```
ASA5520# show capture
capture CAP-TESTE interface Inside access-list ANY [Buffer Full - 522885 bytes]
ASA5520# show capture CAP-TESTE

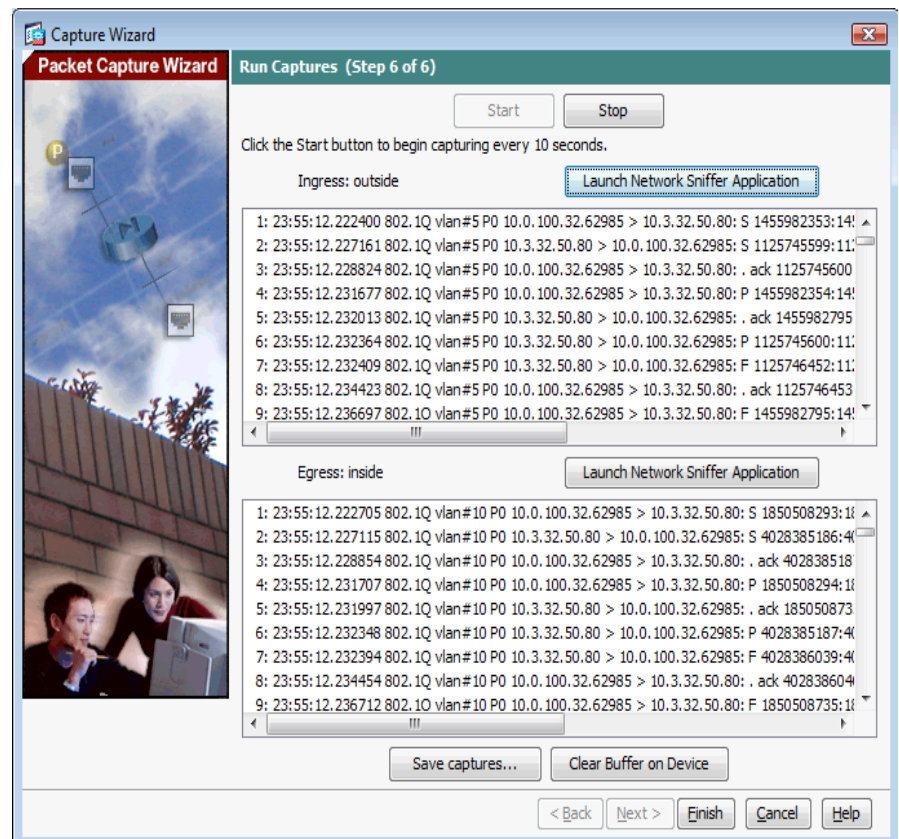
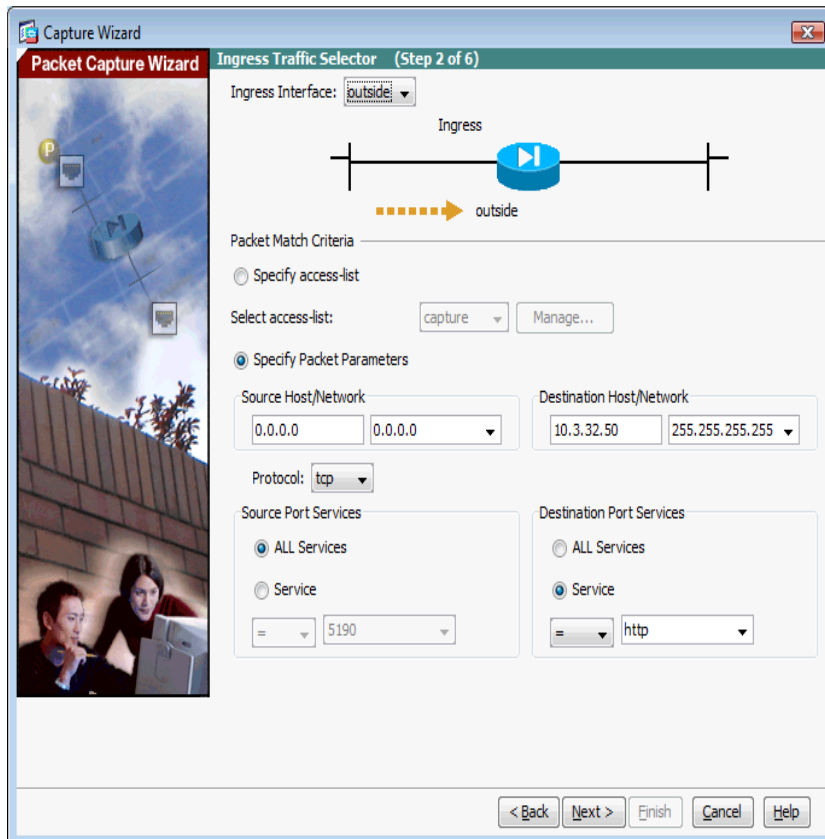
1188 packets captured

  1: 11:23:23.484883 10.97.13.14.1120 > 10.97.13.19.49: S 831343507:831343507(0) win 32768 <mss
1380,sackOK,nop,nop,nop,nop,timestamp 240357987 0>
  2: 11:23:23.485173 10.97.13.14.443 > 10.134.8.77.51179: P 2467161570:2467161740(170) ack 1656230729 win 32768
  3: 11:23:23.485311 10.97.13.19.49 > 10.97.13.14.1120: S 4292803559:4292803559(0) ack 831343508 win 16384 <mss
1460,nop,nop,timestamp 0 0,nop,nop,sackOK>
  4: 11:23:23.485372 10.97.13.14.1120 > 10.97.13.19.49: . ack 4292803560 win 32768 <nop,nop,timestamp 240357988 0>
  5: 11:23:23.485433 10.97.13.14.443 > 10.134.8.77.51179: P 2467161740:2467161875(135) ack 1656230729 win 32768
  6: 11:23:23.485555 10.97.13.14.1120 > 10.97.13.19.49: P 831343508:831343634(126) ack 4292803560 win 32768
<nop,nop,timestamp 240357988 0>
  7: 11:23:23.485616 10.97.13.14.443 > 10.134.8.77.51179: P 2467161875:2467162056(181) ack 1656230729 win 32768
  8: 11:23:23.485982 10.97.13.19.49 > 10.97.13.14.1120: R 4292803560:4292803560(0) ack 831343634 win 0
  9: 11:23:23.486714 10.134.8.77.51179 > 10.97.13.14.443: . ack 2467161875 win 16560
 10: 11:23:23.492848 10.97.13.14.52280 > 10.97.13.19.49: S 16596585:16596585(0) win 32768 <mss
1380,sackOK,nop,nop,nop,nop,timestamp 240357995 0>
 11: 11:23:23.493047 10.97.13.14.443 > 10.134.8.77.51179: P 2467162056:2467162226(170) ack 1656230729 win 32768
 12: 11:23:23.493153 10.97.13.14.443 > 10.134.8.77.51179: P 2467162226:2467162368(142) ack 1656230729 win 32768
 13: 11:23:23.493245 10.97.13.14.443 > 10.134.8.77.51179: P 2467162368:2467162551(183) ack 1656230729 win 32768
 14: 11:23:23.493306 10.97.13.19.49 > 10.97.13.14.52280: S 1541279907:1541279907(0) ack 16596586 win 16384 <mss
1460,nop,nop,timestamp 0 0,nop,nop,sackOK>
 15: 11:23:23.493367 10.97.13.14.52280 > 10.97.13.19.49: . ack 1541279908 win 32768 <nop,nop,timestamp 240357996 0>
 16: 11:23:23.493458 10.97.13.14.52280 > 10.97.13.19.49: P 16596586:16596719(133) ack 1541279908 win 32768
<nop,nop,timestamp 240357996 0>
 17: 11:23:23.493977 10.97.13.19.49 > 10.97.13.14.52280: R 1541279908:1541279908(0) ack 16596719 win 0
 18: 11:23:23.494435 10.134.8.77.51179 > 10.97.13.14.443: . ack 2467162226 win 16209
 19: 11:23:23.494572 10.134.8.77.51179 > 10.97.13.14.443: . ack 2467162551 win 15884
 20: 11:23:23.499440 10.97.13.14.61705 > 10.97.13.19.49: S 3345613117:3345613117(0) win 32768 <mss
1380,sackOK,nop,nop,nop,nop,timestamp 240358002 0>
```

Ferramentas

Captura de Pacotes no ASDM

- Para habilitar captura de pacotes no ASDM:
Wizards → Packet Capture Wizard



Ferramentas

Simulador de Pacotes

- Packet-Tracer possibilita fazer um **acompanhamento (“trace”)** de onde e **como os pacotes são processados pelo ASA.**
- Você pode tanto utilizar um **pacote “dummy”** quanto um **pacote real** previamente capturado:

Trace com pacote “dummy”:

```
Pod19# packet-tracer input outside tcp 192.168.1.5 1025 10.3.19.50 80
```

Trace com pacote capturado:

```
Pod19# capture out interface outside access-list cap trace
```

```
Pod19# show capture out
```

```
. . .
```

```
43: 19:30:24.765615 802.1Q vlan#5 P0 10.1.1.211.43730 > 10.3.19.50.80: S  
612034548:612034548(0) win 5840 <mss 1460,sackOK,timestamp 372044700 0,nop,wscale 6>
```

```
Pod19# show capture out trace packet-number 43
```

Ferramentas

Simulador de Pacotes

```
ASA5520-IPS# packet-tracer input inside icmp 192.168.0.1 8 0 10.97.13.14
```


```
Phase: 1  
Type: CAPTURE  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
MAC Access list
```

```
Phase: 2  
Type: ACCESS-LIST  
Subtype:  
Result: ALLOW  
Config:  
Implicit Rule  
Additional Information:  
MAC Access list
```

```
(...)
```

```
Phase: 8  
Type: FLOW-CREATION  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
New flow created with id 241, packet dispatched to next module
```

```
Result:  
input-interface: Inside  
input-status: up  
input-line-status: up  
output-interface: NP Identity Ifc  
output-status: up  
output-line-status: up  
Action: allow
```



Saída do comando
geralmente é extensa!

Ferramentas

Simulador de Pacotes

No ASDM, localizado em
Tools → Packet Tracer

The screenshot displays the Cisco ASDM Packet Tracer interface. At the top, it says "Cisco ASDM Packet Tracer - 10.2.20.2". Below this, there are instructions: "Select the packet type and supply the packet parameters. Click Start to trace the packet." The interface includes several input fields: "Interface" set to "outside", "Packet Type" set to "TCP", "Source IP Address" set to "192.168.1.5", "Destination IP Address" set to "10.3.20.50", "Source Port" set to "1025", and "Destination Port" set to "80". There are "Start" and "Clear" buttons. A "Show animation" checkbox is checked. Below this is a flow diagram showing the packet's path through various processing stages: outside, UN-NAT skip, Access list Lookup, IP Options Lookup, HOST-LIMIT, NAT Lookup, NAT Lookup, IP Options Lookup, Flow creation, and inside. Each stage has a green checkmark above it. At the bottom, there is a "Phase" section with a table of processing phases and their status:

Phase	Ac...
ACCESS-LIST	✓
FLOW-LOOKUP	✓
UN-NAT	✓
ACCESS-LIST	✓
IP-OPTIONS	✓

The "UN-NAT" phase is expanded, showing the following configuration:

```
Type - UN-NAT Subtype - static Action - ALLOW Show rule in NAT Rules table.

Config
static (inside,outside) 10.3.20.50 10.3.20.50 netmask 255.255.255.255
nat-control
match ip inside host 10.3.20.50 outside any
static translation to 10.3.20.50
translate_hits = 0, untranslate_hits = 4808

Info
NAT divert to egress interface inside
Untranslate 10.3.20.50/0 to 10.3.20.50/0 using netmask 255.255.255.255
```

At the bottom of the window, there are "Close" and "Help" buttons.

Terceira Pergunta

Dentre as ferramentas apresentadas, qual seria a mais adequada para visualizar o processamento de um determinado pacote no ASA?

- a) Syslog.**
- b) Tabela de Conexões (“show conn”).**
- c) Captura de Pacotes (“capture”).**
- d) Simulador de Pacotes (“packet-tracer”).**

Faça suas perguntas agora!

Use o painel de perguntas e respostas (Q&A) para perguntar ao especialista agora. Ele começará a responder.



Perguntas e Respostas

O Especialista responderá às questões verbalmente. Use o painel escrito Q&A para continuar fazendo suas perguntas.



Queremos sua opinião!

Aqueles que preencherem o questionário de avaliação entrarão em um sorteio para ganhar:

Um vale presente

Para fazer a avaliação, favor clicar no endereço fornecido no chat ou no pop-up quando o evento terminar.

Evento Pergunte ao Especialista (com Davi Garcia)

Se tiver perguntas adicionais, poderá perguntar ao especialista. Ele estará respondendo até o dia 7 de Setembro.

<https://supportforums.cisco.com/community/portuguese/canto-dos-especialistas/ask-the-expert>

Você poderá assistir ao vídeo ou ler as perguntas e respostas 5 dias úteis após o evento em

<https://supportforums.cisco.com/community/portuguese/canto-dos-especialistas/webcasts>



Próximo evento – Pergunte ao Especialista

Tema: Gravação de chamadas no Cisco Unified Communications Manager



Com a Especialista Cisco :**Bianca Meslin**

Tire dúvidas sobre como configurar o Call Manager e os telefones para gravação de chamadas

Este evento ocorrerá do dia 10 de Setembro ao dia 21

Acesse

<https://supportforums.cisco.com/community/portuguese/canto-dos-especialistas/ask-the-expert>

Próximo Webcast – Em inglês

Tema: Cable Modem Termination Systems (CMTS): Arquitetura, Configuração e Troubleshooting



Quarta-feira 12 de Setembro,
12:00 p.m. Brasília
4:00 p.m. Lisboa
5:00 p.m. Paris

Junte-se ao Especialista Cisco:

Eric Bautista

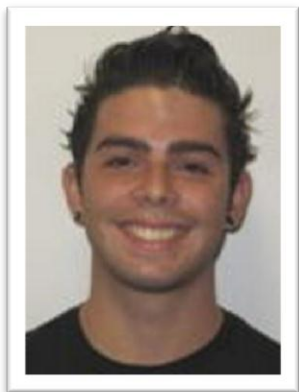
Durante este evento ao vivo você terá uma visão geral do Cable Modem Termination System e aprenderá as configurações básicas e como solucionar problemas comuns

Registre-se neste webcast através do endereço

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

Próximo Webcast – Em espanhol

Tema: Cisco ASA Post 8.3 NAT Configuration



Quarta-feira 12 de Setembro,
12:00 p.m. Brasília
4:00 p.m. Lisboa
5:00 p.m. Paris

Junte-se ao Especialista Cisco:

Julio Carvajal

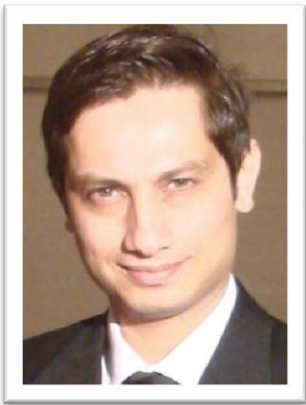
Durante este evento ao vivo você aprenderá sobre as mudanças básicas a fim de atualizar o Software Cisco IOS em um ASA para a versão 8.3 ou mais atual. Julio também explicará a configuração do route monitoring com SLA através do ASA e outros cenários comuns.

Registre-se neste webcast através do endereço

http://tools.cisco.com/gems/cust/customerQA.do?METHOD=E&LANGUAGE_ID=S&PRIORITY_CODE=4&SEMINAR_CODE=S17005

Webcast em Outubro- Inglês

Tema: Troubleshooting SSL VPN no ASA



Terça-feira 9 de Outubro

12:00 p.m. Brasília

4:00 p.m. Lisboa

5:00 p.m. Paris

Junte-se ao Especialista Cisco:

Jazib Frahim

Durante este evento ao vivo você aprenderá como solucionar problemas de SSL VPN no ASA

O registro para este webcast estará disponível em Setembro em

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

Pergunte aos Especialistas – Em Inglês



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

Com o Especialista Cisco: **Ron Hanson**

Tire dúvidas de como configurar, operar e solucionar problemas do RF Gateway 1



Tema: Intrusion Prevention System (IPS)

Com o Especialista Cisco : **Robert Albach**

Tire dúvidas de como configurar e solucionar problemas do IPS.



Tema: Preparing Cisco Unified Communications Manager 8.x to Support Cisco Jabber for Android/iPhone

Com o Especialista Cisco : **Rajamani Nallakaruppan**

Aprenda a preparar o Cisco Unified Communications Manager 8.x para suportar Cisco Jabber para Android/iPhone (este evento acontece até 28 de Agosto)

Participe das discussões com esses especialistas em:

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

Pergunte aos Especialistas– Próximo mês – em Inglês

Tema: Conceitos, Configuração e Troubleshooting Layer 2 MPLS VPN – Any Transport over MPLS (AToM)



Com o Especialista Cisco : **Vignesh R. P.**

Aprenda, pergunte e esclareça qualquer questão sobre conceito, configuração e Troubleshooting Layer 2 MPLS VPN – Any Transport over MPLS (AToM).

Participe da discussão neste evento Pergunte ao Especialista:

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

(Este evento ocorre de 10 de Setembro até 21 de Setembro)

Fórum do Facebook e Pergunte ao Especialista - Inglês

Tema: Migration Best Practices for ASA 8.3/8.4



Terça-Feira 6 de Setembro

1:00 p.m. Brasília

5:00 p.m. Lisboa, Portugal

Junte-se ao Especialista Cisco:

Praveena Shanubhogue

Aprenda sobre as melhores práticas que devem ser tomadas com cuidado ao migrar da versão 8.2 ou anterior para 8.3 ou posterior. Faça perguntas sobre novas funcionalidades introduzidas, entenda bugs ou problemas conhecidos que é preciso estar atento ao migrar da versão 8.2 para 8.3 ou posterior.

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

Este evento estará disponível do dia 6 de Setembro até 14 de Setembro em

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

Convidamos você a participar da CSC em português e em nossas redes sociais

<https://supportforums.cisco.com/community/portuguese>



Portugal: <http://www.facebook.com/ciscoportugal>

Brasil: <http://www.facebook.com/CiscoDoBrasil>



Portugal: <https://twitter.com/CiscoPortugal>

Brasil: <http://twitter.com/CiscoDoBrasil>



Portugal: <http://www.youtube.com/user/ciscoportugal>

Brasil: <http://www.youtube.com/user/ciscoDoBrasilTV>



Portugal: <http://ciscoportugalblog.wordpress.com/>

Temos comunidades em outros idiomas

Se você fala **Espanhol**, **Japonês**, **Russo** ou **Polonês**, convidamos você a tirar suas dúvidas e colaborar nas comunidades desses idiomas.

- Espanhol → <https://supportforums.cisco.com/community/spanish>
- Japonês → <https://supportforums.cisco.com/community/csc-japan>
- Polonês → <https://supportforums.cisco.com/community/etc/netpro-polska>
- Russo → <https://supportforums.cisco.com/community/russian>

Obrigado pela
sua presença

Por favor complete o formulário de avaliação do evento e
ganhe prêmios



Thank you.

