Nova visão de Listas de Acesso Cisco CBAC e ZPF

Prof.Celso Rabelo M Pinto

Centro Universitário da Cidade

27/02/2012

Visão Geral

- ACLs executam testes até que determinada condição seja verdadeira;
- Última condição implícita é um deny any;
- Quando aplicadas em interfaces permitem a filtragem de pacotes;
- Por interface, são permitidas 2 acls por protocolo de camada 3 (in out);
- Podem ser aplicadas em mapas de roteamento, e em outras aplicações.

ACLs Tradicionais

- Podem ser de 2 tipos: padrão e estendida
- Na padrão só é levado em consideração o endereçamento de origem, deve ser aplicada o mais próximo possível do destino
- Na estendida é levando em consideração origem, destino e tipo de protocolo, deve ser colocada o mais próximo da origem, mas limitar tráfego não interessante

ACL padrão exemplo

- Router(config)access-list 1 permit 10.0.0.0 0.0.0.255
- Router(config-if)ip address 10.0.1.1 255.255.255.0
- Router(config-if)ip access-group 1 out
- Permite que hosts da rede 10.0.0.0/24 acessem estações da rede 10.0.1.0/24

ACL Estendida - exemplo

- Router(config)access-list 100 permit ip 10.0.0.0 0.0.0.255 10.0.1.0 0.0.0.255
- Router(config-if)ip address 10.0.0.1 255.255.255.0
- Router(config-if)ip access-group 100 in
- Permite que hosts da rede 10.0.0.0/24 acessem estações da rede 10.0.1.0/24

ACLs Complexas

- Incluem funcionalidades as acls anteriores, de acordo com a necessidade apresentada
- Temporal: funcionam por um período de tempo determinado
- Reflexiva: permitem o fluxo de dados somente em um sentido
- Dinâmica: após a autenticação do usuário, a acl funciona por um determinado período de tempo

ACL Temporal

Etapa 1	`R1(config)#time-range EVERYOTHERDAY` `R1(config-time-range)#periodic Monday Wednesday Friday 8:00 to 17:00`
Etapa 2	`R1(config)#access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range EVERYOTHERDAY`
Etapa 3	`R1(config)#interface s0/0/0` `R1(config-if)#ip access-group 101 out`

ACL Reflexiva

Etapa 1

```
R2(config)#ip access-list extended OUTBOUNDFILTERS
R2(config-ext-nacl)# permit tcp 192.168.0.0 0.0.255.255
any reflect TCPTRAFFIC
R2(config-ext-nacl)# permit icmp 192.168.0.0 0.0.255.255
any reflect ICMPTRAFFIC
```

Etapa 2

```
R2(config)#ip access-list extended INBOUNDFILTERS
R2(config-ext-nacl)# evaluate TCPTRAFFIC
R2(config-ext-nacl)# evaluate ICMPTRAFFIC
```

Etapa 3

```
R2(config)#interface S0/1/0
R2(config-if)#ip access-group INBOUNDFILTERS in
R2(config-if)#ip access-group OUTBOUNDFILTERS out
```

ACL Dinâmica

Etapa 1	`R3(config)#username Student password 0 cisco`
Etapa 2	`R3(config)# access-list 101 permit tcp any host 10.2.2.2 eq telnet` `R3(config)#access-list 101 dynamic testlist timeout 15 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255`
Etapa 3	`R3(config)#interface serial 0/0/1` `R3(config-if)#ip access-group 101 in`

Etapa 4	`R3(config)#line vty 0 4`
	`R3(config-line)#login local`
	`R3(config-line)# autocommand access-enable host timeout 5`

ACLs Compiladas

- Permite que roteadores das séries 7200 ou superiores uma abordagem diferenciada para melhorar o desempenho
- As acls são compiladas em tabelas, e as consultas são feitas de forma diferente da sequencial

ACLs Compiladas - Exemplo

- Router(config)access-list compiled
- Router(config) access-list 1 deny any
- Router(config) access-list 2 deny 192.168.0.0 0.0.0.255
- Router(config) access-list 2 permit any
- A primeira linha ativa o modo de compilação

Visão Geral

- Regras normais de acl só levam em consideração a porta de serviço e não o serviço propriamente dito
- ACLs reflexivas criam um fluxo de dados, mas continua sem verificar a camada de aplicação (assinatura)
- Solução: analisar o comportamento do pacote ao passar pelo roteador

CBAC - visão geral

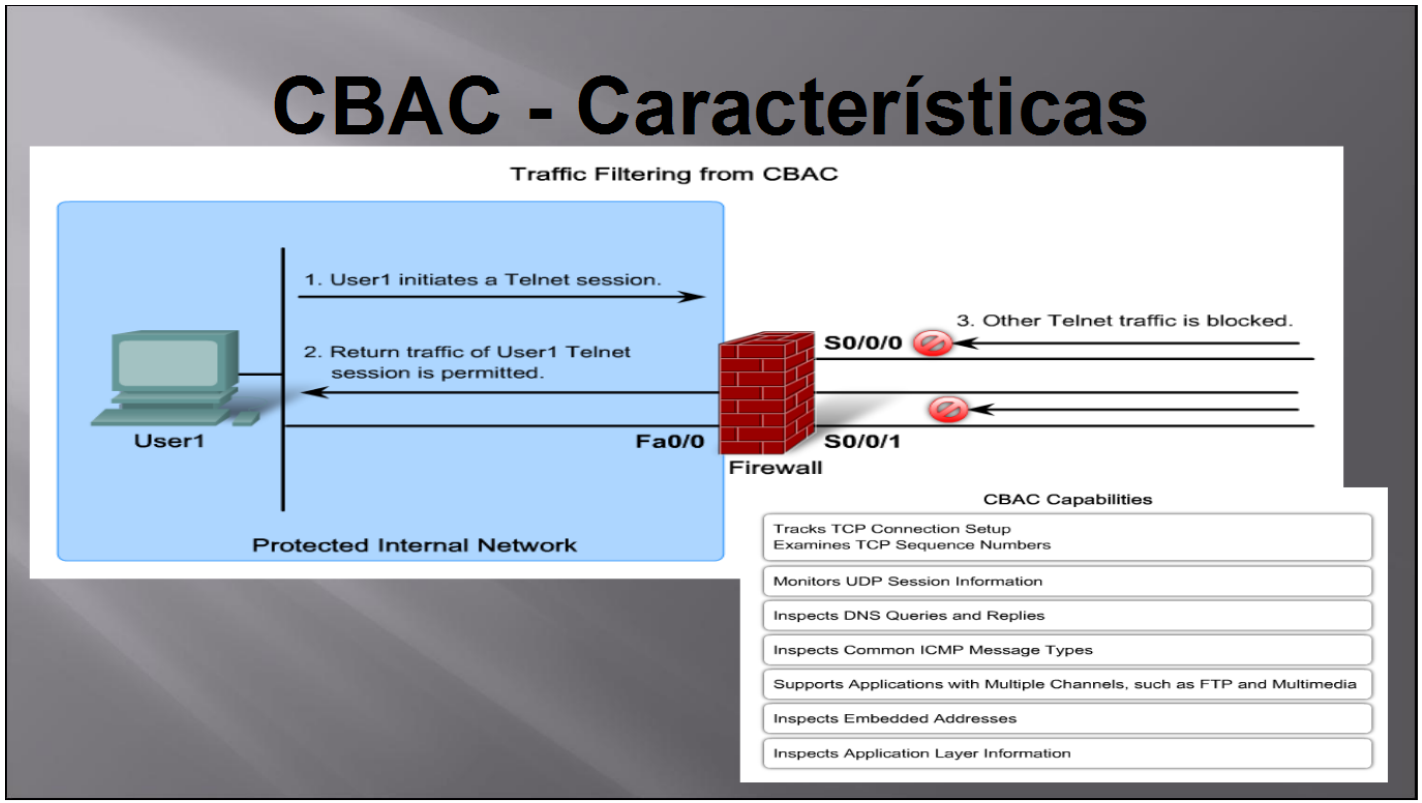
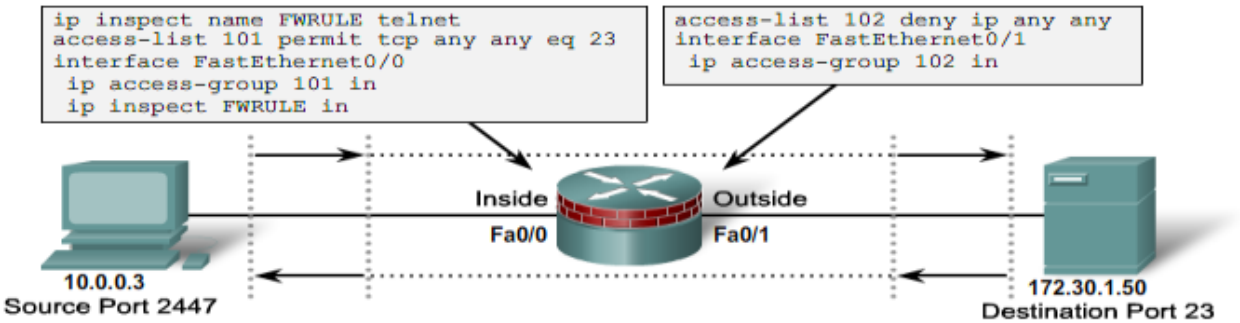


Figura: Visão

CBAC - Como implementar

- Definição das interfaces em relação ao posicionamento (interno ou externo)
- Criação das ACLs para atender os fluxos
- Criação das inspeções
- O CBAC cria como se fosse uma ACL dinâmica do fluxo externo para o interno

CBAC - Exemplo



The TCP traffic is inspected by FWRULE.

1. `ip inpsect FWRULE in`

The firewall creates a dynamic ACL allowing return traffic back through the firewall.

2. `access-list 102 permit tcp host 172.30.1.50 eq 23 host 10.0.0.3 eq 2447`

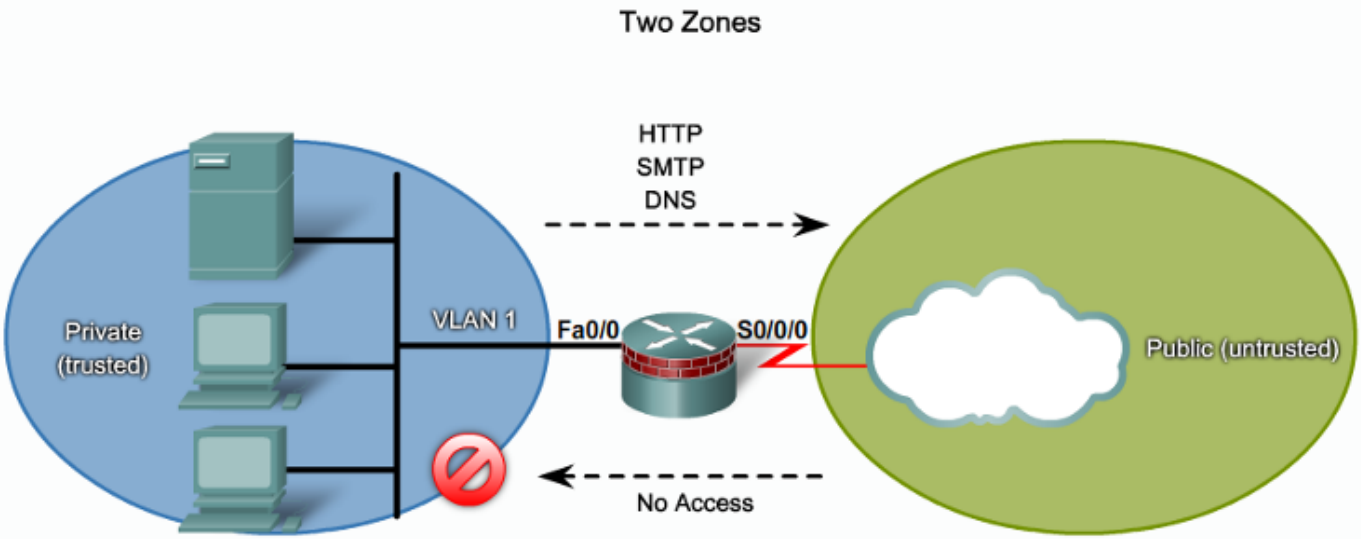
3. The firewall continues to inspect control traffic and dynamically creates and removes ACLs as required by the application. It also monitors and protects against application-specific attacks.

4. The firewall detects when an application terminates or times out and removes all dynamic ACLs for that session.

ZPF - visão geral

- Nesta implementação a primeira coisa a ser realizada é a definição das zonas.
- As interfaces são inseridas às zonas
- Em seguida é criado um conjunto de testes chamado classe, dentro dessa classe pode haver ACLs
- Esta classe é inserida a uma política, que define o que será feito
- Essa política é inserida a um par de zonas
- As interfaces são inseridas as zonas pré-definidas

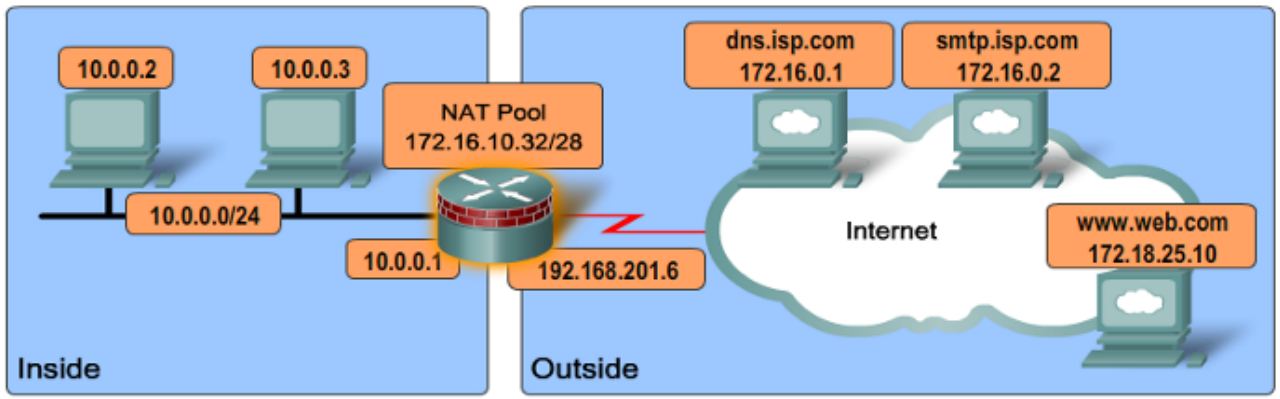
ZPF - Definição de Zonas



- The private zone must reach the Internet, with access to HTTP, SMTP, and DNS services.
- The public zone should not have any inbound access.

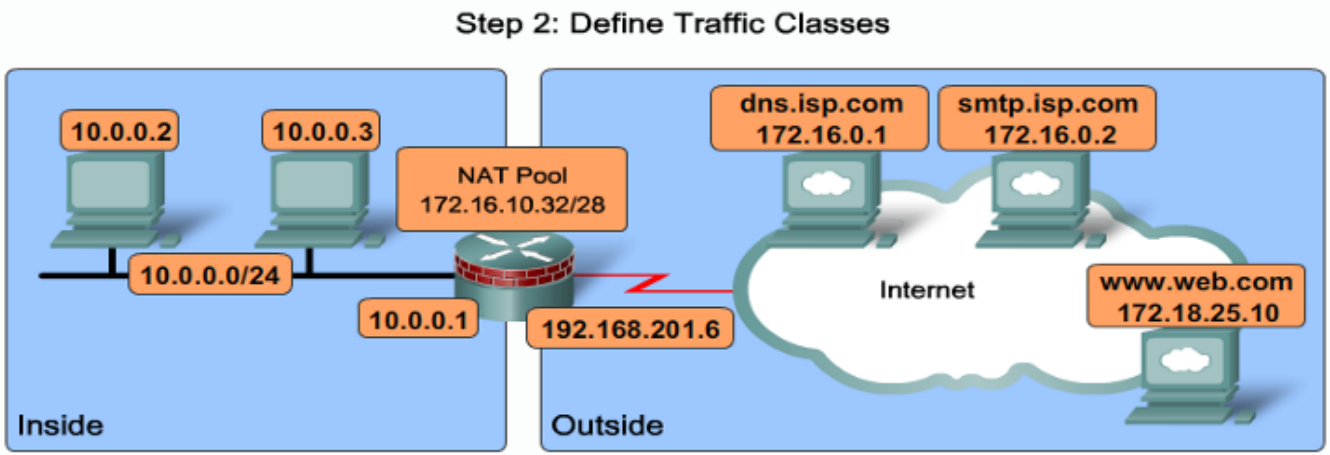
ZPF - Criação de Zonas

Step 1: Create Zones




```
FW(config)# zone security Inside
FW(config-sec-zone)# description Inside network
FW(config)# zone security Outside
FW(config-sec-zone)# description Outside network
```

ZPF - Criação de Classes

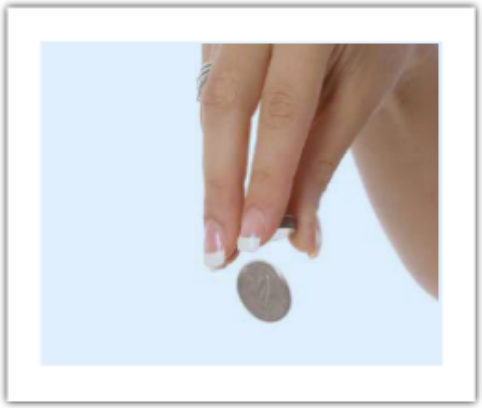



```
FW(config)# class-map type inspect FOREXAMPLE
FW(config-cmap)# match access-group 101
FW(config-cmap)# exit
FW(config)# access-list 101 permit ip 10.0.0.0 0.0.0.255 any
```

ZPF - O que as políticas fazem

ZPF Actions

Inspect



Drop

Pass

ZPF - Ações das Políticas

Ações das políticas

Zone-Based Policy Firewall Rules for Application Traffic

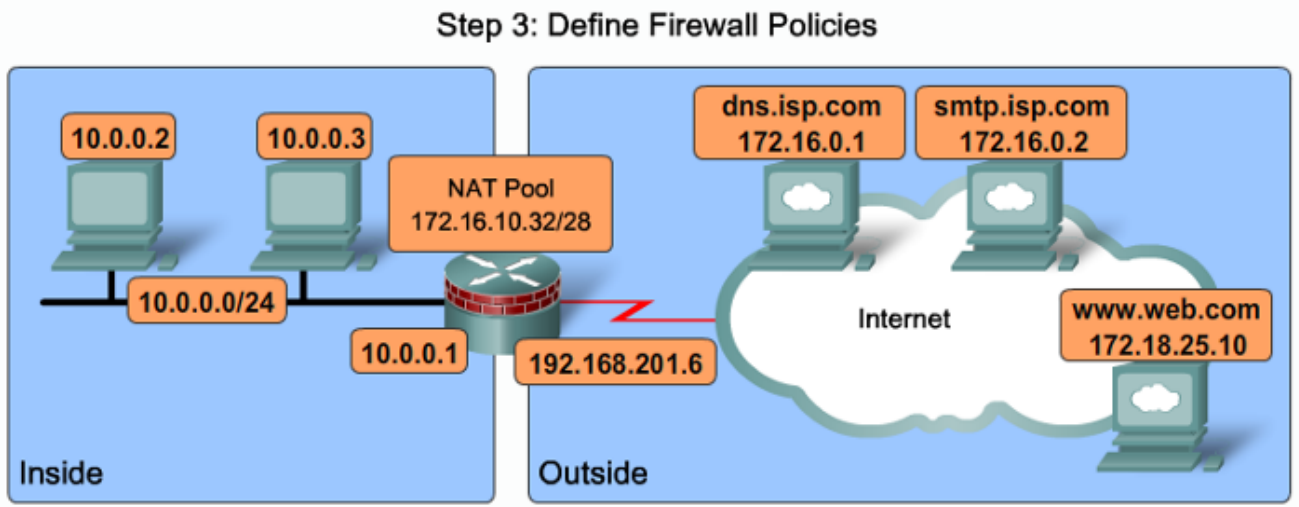
The source policy application and default policy for traffic is applied according to these rules:

Source interface member of zone?	Destination interface member of zone?	Zone pair exists?	Policy exists?	RESULT
NO	NO	N/A	N/A	No impact of zoning/policy
YES (zone 1)	YES (zone 1)	N/A*	N/A	No policy lookup (PASS)
YES	NO	N/A	N/A	DROP
NO	YES	N/A	N/A	DROP
YES (zone 1)	YES (zone 2)	NO	N/A	DROP
YES (zone 1)	YES (zone 2)	YES	YES	policy actions

Zone-Based Policy Firewall Rules for Router Traffic

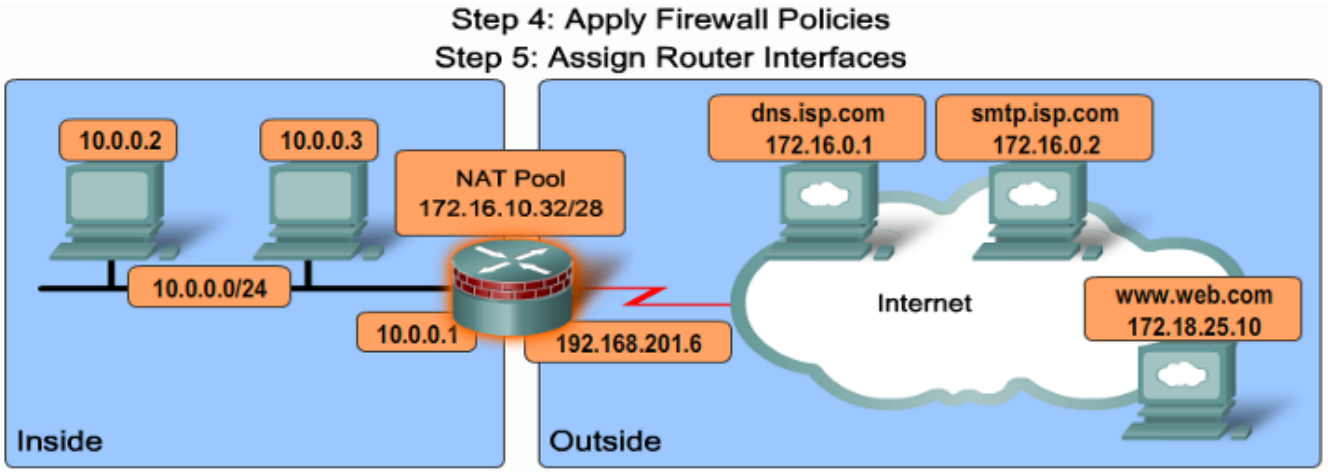
Source interface member of zone?	Destination interface member of zone?	Zone pair exists?	Policy exists?	Result
ROUTER	YES	NO	N/A	PASS
ROUTER	YES	YES	NO	PASS
ROUTER	YES	YES	YES	policy actions
YES	ROUTER	NO	N/A	PASS
YES	ROUTER	YES	NO	PASS
YES	ROUTER	YES	YES	policy actions

ZPF - Criação de Políticas




```
FW(config)# policy-map type inspect InsideToOutside
FW(config-pmap)# class type inspect FOREXAMPLE
FW(config-pmap-c)# inspect
```

ZPF - Associação de política a zonas




```
FW(config)# zone-pair security InsideToOutside source Inside destination Outside
FW(config-sec-zone-pair)# description Internet Access
FW(config-sec-zone-pair)# service-policy type inspect InsideToOutside
FW(config-sec-zone-pair)# interface F0/0
FW(config-if)# zone-member security Inside
FW(config-if)# interface S0/0/0.100 point-to-point
FW(config-if)# zone-member security Outside
```

ZPF - Exemplo

```
hostname FW1
!(cria regras de inspeção, no caso testam a acl 100)
class-map type inspect match-all regras
 match access-group 100
!(associa regras a uma política)
policy-map type inspect firewall
 class type inspect regras
 inspect
!(cria as zonas do firewall)
zone security IN
zone security OUT
!(cria um par de zonas e associa um política a ela)
zone-pair security teste source IN destination OUT
 service-policy type inspect firewall
interface FastEthernet0/0
 ip address 192.168.0.1 255.255.255.0
!(vincula uma zona a uma interface)
 zone-member security IN
 duplex auto
 speed auto
 no shut
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
!(vincula uma zona a uma interface)
 zone-member security OUT
 duplex auto
 speed auto
 no shut
interface Vlan1
 no ip address
```

Bibliografia

- http://www.celsorabelo.eti.br/
- Cisco Firewalls - Concepts, Design and Deployment for Cisco Statful solutions
- CCNA Security - Official Exam Certification Guide