# PANCADINHA dinâmica ASA 8.3(x) com dois redes internas e exemplos de configuração do Internet

## Índice



## Introdução

Este documento fornece uma configuração de exemplo para a PANCADINHA dinâmica em uma ferramenta de segurança adaptável de Cisco (ASA) essa versão de software das corridas 8.3(1). A PANCADINHA dinâmica traduz endereços reais múltiplos a um único endereço IP de Um ou Mais Servidores Cisco ICM NT traçado traduzindo o endereço e a porta de origem de origem real ao endereço traçado e à porta traçada original. Cada conexão exige uma sessão de tradução separada, pois a porta de origem difere para cada conexão.

## Pré-requisitos

### Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Certifique-se que a rede interna tem duas redes situadas no interior do ASA:192.168.0.0/24 — Rede conectada diretamente ao ASA.192.168.1.0/24 — Rede no interior do ASA, mas atrás de um outro dispositivo (por exemplo, um roteador).
- Certifique-se dos usuários internos obter a PANCADINHA como segue:Os anfitriões na sub-rede 192.168.1.0/24 obterão a PANCADINHA a um endereço IP de Um ou Mais Servidores

Cisco ICM NT de reposição dado pelo ISP (10.1.5.5).Todo o outro host atrás do interior do ASA obterá a PANCADINHA ao endereço IP de Um ou Mais Servidores Cisco ICM NT da interface externa do ASA (10.1.5.1).

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Ferramenta de segurança adaptável de Cisco (ASA) com versão 8.3(1)
- Versão 6.3(1) ASDM

**Nota:** Consulte Habilitação de Acesso HTTPS para o ASDM para permitir que o ASA seja configurado pelo ASDM.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Refira as convenções dos dicas técnicas da Cisco para obter informações sobre das convenções de documento.

# Configuração

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

**Nota:** Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918, que foram usados em um ambiente de laboratório.

- Configuração do ASA via CLI
- Configuração ASDM

## Configuração do ASA via CLI

Este documento utiliza as configurações mostradas abaixo.

| Configuração dinâmica da PANCADINHA ASA |
| --- |
| ASA#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. *!--- Creates an object called OBJ_GENERIC_ALL. !--- Any host IP not already matching another configured !--- object will get PAT to the outside interface IP !--- on the ASA (or 10.1.5.1), for internet bound traffic.* ASA(config)#**object network OBJ_GENERIC_ALL** ASA(config-obj)#**subnet 0.0.0.0 0.0.0.0** ASA(config-obj)#**exit** ASA(config)#**nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface** *!--- The above* |

*statements are the equivalent of the !--- nat/global combination (as shown below) in v7.0(x), !--- v7.1(x), v7.2(x), v8.0(x), v8.1(x) and v8.2(x) ASA code:* **nat (inside) 1 0.0.0.0 0.0.0.0 global (outside) 1 interface** *!--- Creates an object called OBJ_SPECIFIC_192-168-1-0. !--- Any host IP facing the the 'inside' interface of the ASA !--- with an address in the 192.168.1.0/24 subnet will get PAT !--- to the 10.1.5.5 address, for internet bound traffic.* ASA(config)#**object network OBJ_SPECIFIC_192-168-1-0** ASA(config-obj)#**subnet 192.168.1.0 255.255.255.0** ASA(config-obj)#**exit** ASA(config)#**nat (inside,outside) source dynamic OBJ_SPECIFIC_192-168-1-0 10.1.5.5** *!--- The above statements are the equivalent of the nat/global !--- combination (as shown below) in v7.0(x), v7.1(x), v7.2(x), v8.0(x), !--- v8.1(x) and v8.2(x) ASA code:* **nat (inside) 2 192.168.1.0 255.255.255.0 global (outside) 2 10.1.5.5**

## Configuração sendo executado ASA 8.3(1)

ASA#**show run** : Saved : ASA Version 8.3(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 10.1.5.1 255.255.255.0 *!--- Configure the inside interface.* ! interface GigabitEthernet0/1 nameif inside security-level 100 ip address 192.168.0.1 255.255.255.0 ! 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:/asa831-k8.bin ftp mode passive **object network OBJ_SPECIFIC_192-168-1-0 subnet 192.168.1.0 255.255.255.0 object network OBJ_GENERIC_ALL subnet 0.0.0.0 0.0.0.0** pager lines 24 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-631.bin no asdm history enable arp timeout 14400 **nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface nat (inside,outside) source dynamic OBJ_SPECIFIC_192-168-1-0 10.1.5.5** route inside 192.168.1.0 255.255.255.0 192.168.0.254 1 route outside 0.0.0.0 0.0.0.0 10.1.5.2 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
```

## Configuração ASDM

A fim terminar esta configuração através da relação ASDM, você deve:

1. Adicionar três objetos de rede; este os exemplos adicionam estes objetos de rede:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. Crie duas regras NAT/PAT; este os exemplos criam regras NAT para estes objetos de rede:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

### Adicionar objetos de rede

Termine estas etapas a fim adicionar objetos de rede:

1. Entre ao ASDM, e escolha a **configuração > o Firewall > os objetos > os objetos de rede/grupos**.
2. Escolha **adicionam > objeto de rede** a fim adicionar um objeto de rede.A caixa de diálogo do objeto de rede adicionar aparece.
3. Incorpore esta informação à caixa de diálogo do objeto de rede adicionar:Nome do objeto de rede. (Este exemplo usa *OBJ_GENERIC_ALL*.)Objeto do tipo de rede. (Este exemplo usa a *rede*.)Endereço IP de Um ou Mais Servidores Cisco ICM NT para o objeto de rede. (Este exemplo usa *0.0.0.0*.)Máscara de rede para o objeto de rede. (Este exemplo usa *0.0.0.0*.)
4. Clique em **OK**.O objeto de rede é criado e aparece na lista dos objetos de rede/grupos, segundo as indicações desta imagem:
5. Repita as etapas precedentes a fim adicionar um segundo objeto de rede, e clique a **APROVAÇÃO**.Este exemplo usa estes valores:Nome: *OBJ_SPECIFIC_192-168-1-0*Digite: *Rede*Endereço IP: *192.168.1.0*Máscara de rede: *255.255.255.0*O segundo objeto é criado e aparece na lista dos objetos de rede/grupos, segundo as indicações desta imagem:
6. Repita as etapas precedentes a fim adicionar um terceiro objeto de rede, e clique a **APROVAÇÃO**.Este exemplo usa estes valores:Nome: *10.1.5.5*Digite: *Host*Endereço IP: *10.1.5.5*Os terceiros objetos de rede são criados e aparecem na lista dos objetos de rede/grupos.A lista dos objetos de rede/grupos deve agora incluir os três objetos exigidos necessários para que as regras NAT provejam.

### Crie regras NAT/PAT

Termine estas etapas a fim criar regras NAT/PAT:

1. Crie a primeira regra NAT/PAT:No ASDM, escolha a **configuração > o Firewall > as regras NAT**, e o clique **adiciona**.A caixa de diálogo da regra adicionar NAT aparece.Nos critérios de verificação de repetição de dados: A área do pacote original da caixa de diálogo da regra adicionar NAT, escolhe **para dentro da** lista de drop-down da interface de origem.Clique a consultação (**...**) abotoe ficado situado à direita do campo de texto do endereço de origem.A caixa de diálogo do endereço de fonte original da consultação aparece.Na caixa de diálogo do endereço de fonte original da consultação, escolha o primeiro objeto de rede que você

criou. (Para este exemplo, escolha **OBJ_GENERIC_ALL**.)Clique o **endereço de fonte original**, e clique a **APROVAÇÃO**.O objeto de rede *OBJ_GENERIC_ALL* aparece agora no campo de endereço de origem nos critérios de verificação de repetição de dados: Área do pacote original da caixa de diálogo da regra adicionar NAT.Na ação: A área traduzida do pacote da caixa de diálogo da regra adicionar NAT, escolhe a **PANCADINHA dinâmica (couro cru) do** tipo caixa de diálogo da fonte NAT.Clique a consultação (**…**) abotoe ficado situado à direita do campo de endereço de origem.A caixa de diálogo traduzida consultação do endereço de origem aparece.Na consultação a caixa de diálogo traduzida do endereço de origem, escolhe o objeto da **interface externa**. (Esta relação tem sido criada já porque é parte da configuração original.)**Endereço de origem traduzido** clique, e **APROVAÇÃO do** clique.A interface externa aparece agora no campo de endereço de origem na ação: Área traduzida do pacote na caixa de diálogo da regra adicionar NAT.**Nota:** O campo da *interface de destino* igualmente muda à interface externa.Verifique que a primeira regra terminada da PANCADINHA aparece como segue:Nos critérios de verificação de repetição de dados: A área do pacote original, verifica estes valores:Interface de origem = para dentroEndereço de origem = OBJ_GENERIC_ALLEndereço de destino = algunsServiço = algunsNa ação: A área traduzida do pacote, verifica estes valores:Tipo da fonte NAT = PANCADINHA dinâmica (couro cru)Endereço de origem = foraEndereço de destino = originalServiço = originalClique em **OK**.A primeira regra NAT aparece no ASDM, segundo as indicações desta imagem:

2. Crie a segunda regra NAT/PAT:No ASDM, escolha a **configuração > o Firewall > as regras NAT**, e o clique **adiciona**.Nos critérios de verificação de repetição de dados: A área do pacote original da caixa de diálogo da regra adicionar NAT, escolhe **para dentro da** lista de drop-down da interface de origem.Clique a consultação (**…**) abotoe ficado situado à direita do campo de endereço de origem.A caixa de diálogo do endereço de fonte original da consultação aparece.Na caixa de diálogo do endereço de fonte original da consultação, escolha o segundo objeto que você criou. (Para este exemplo, escolha **OBJ_SPECIFIC_192-168-1-0**.)Clique o **endereço de fonte original**, e clique a **APROVAÇÃO**.O objeto de rede *OBJ_SPECIFIC_192-168-1-0* aparece no campo de endereço de origem nos critérios de verificação de repetição de dados: Área do pacote original da caixa de diálogo da regra adicionar NAT.Na ação: A área traduzida do pacote da caixa de diálogo da regra adicionar NAT, escolhe a **PANCADINHA dinâmica (couro cru) do** tipo caixa de diálogo da fonte NAT.Clique**… o** botão situado à direita do campo de endereço de origem.A caixa de diálogo traduzida consultação do endereço de origem aparece.Na consultação a caixa de diálogo traduzida do endereço de origem, escolhe o objeto de **10.1.5.5**. (Esta relação tem sido criada já porque é parte da configuração original).Clique o **endereço de origem traduzido**, e clique então a **APROVAÇÃO**.O objeto de rede de **10.1.5.5** aparece no campo de endereço de origem na ação: Área traduzida do pacote da caixa de diálogo da regra adicionar NAT.Nos critérios de verificação de repetição de dados: A área do pacote original, escolhe **fora da** lista de drop-down da interface de destino.**Nota:** Se você não escolhe *fora* para esta opção, a interface de destino proverá *alguns*.Verifique que a segunda regra terminada NAT/PAT aparece como segue:Nos critérios de verificação de repetição de dados: A área do pacote original, verifica estes valores:Interface de origem = para dentroEndereço de origem = OBJ_SPECIFIC_192-168-1-0Endereço de destino = foraServiço = algunsNa ação: A área traduzida do pacote, verifica estes valores:Tipo da fonte NAT = PANCADINHA dinâmica (couro cru)Endereço de origem = 10.1.5.5Endereço de destino = originalServiço = originalClique em **OK**.A configuração de NAT terminada aparece no ASDM, segundo as indicações desta imagem:

3. Clique o **botão Apply Button** a fim aplicar as mudanças à configuração running.

Isto termina a configuração da PANCADINHA dinâmica em uma ferramenta de segurança adaptável de Cisco (ASA).

# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

## Verificando a regra genérica da PANCADINHA

- host local da mostra — Mostra os estados da rede dos host locais.
```
ASA#show local-host
Interface outside: 1 active, 2 maximum active, 0 denied local host: <125.252.196.170>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited !--- The TCP connection outside address corresponds !--- to the actual destination of 125.255.196.170:80 Conn: TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:03, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04, bytes 11896, flags UIO Interface inside: 1 active, 1 maximum active, 0 denied local host: <192.168.0.5>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited !--- The TCP PAT outside address corresponds to the !--- outside IP address of the ASA – 10.1.5.1. Xlate: TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags ri idle 0:00:17 timeout 0:00:30 TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags ri idle 0:00:17 timeout 0:00:30 Conn: TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:03, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04, bytes 11896, flags UIO
```
- show conn — Mostra o estado de conexão para o tipo de conexão designado.
```
ASA#show conn 2 in use, 3 most used TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:06, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:01, bytes 13526, flags UIO
```
- xlate da mostra — Mostra a informação sobre os slots de tradução.
```
ASA#show xlate 4 in use, 7 most used Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity, T - twice TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags ri idle 0:00:23 timeout 0:00:30 TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags ri idle 0:00:23 timeout 0:00:30
```

## Verificando a regra específica da PANCADINHA

- host local da mostra — Mostra os estados da rede dos host locais.
```
ASA#show local-host
Interface outside: 1 active, 2 maximum active, 0 denied local host: <125.252.196.170>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited !--- The TCP connection outside address corresponds to !--- the actual destination of 125.255.196.170:80. Conn: TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03, bytes 11896, flags UIO Interface inside: 1 active, 1 maximum active, 0 denied local host: <192.168.0.5>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited !--- The TCP PAT outside address corresponds to an !--- outside IP address of 10.1.5.5. Xlate: TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags ri idle 0:00:17 timeout 0:00:30 TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/23673 flags ri idle 0:00:17 timeout 0:00:30 Conn: TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03, bytes 11896, flags UIO
```

- show conn — Mostra o estado de conexão para o tipo de conexão designado.ASA#**show conn** 2 in use, 3 most used TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07, bytes 13653, flags UIO TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03, bytes 13349, flags UIO
- xlate da mostra — Mostra a informação sobre os slots de tradução.ASA#**show xlate** 3 in use, 9 most used Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity, T - twice TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags ri idle 0:00:23 timeout 0:00:30 TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/29673 flags ri idle 0:00:23 timeout 0:00:30

# Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

# Informações Relacionadas

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems