ASA: Acesso remoto do modo do Multi-contexto (AnyConnect) VPN

Índice

Introdução

Este documento descreve como configurar o Virtual Private Network (VPN) do Acesso remoto (RA) no Firewall adaptável da ferramenta de segurança de Cisco (ASA) no modo do contexto múltiplo (MC). Mostra Cisco ASA no modo de contexto múltiplo apoiado/recursos não suportados e requisito de licenciamento no que diz respeito a RA VPN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de SSL ASA AnyConnect

- Configuração do contexto múltiplo ASA

Componentes Utilizados

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

- Dois código sendo executado ASA 5585 9.5(2)
- Cliente 3.1.10010 de AnyConnect

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, entenda o possível impacto de todos os comandos

Informações de Apoio

o Multi-contexto é um formulário da virtualização que permite a múltiplo cópias independentes de um aplicativo ser executado simultaneamente no mesmo hardware, com cada cópia (ou dispositivo virtual) que aparecem que um dispositivo físico separado ao usuário. Isto permite que um único ASA apareça como ASA múltiplos aos usuários independentes múltiplos. A família ASA apoiou Firewall virtuais desde sua versão inicial; contudo, não havia nenhum apoio da virtualização para o Acesso remoto no ASA. O apoio VPN LAN2LAN (L2L) para o multi-contexto foi adicionado para a liberação 9.0. Do multi-contexto **9.5.2** baseado apoio da virtualização para conexões do Acesso remoto VPN (RA) ao ASA.

Recursos suportados

- Conectividade de AnyConnect 3.X+ SSL (IPv4, IPv6)
- Configuração centralizada da imagem de AnyConnect
- Upgrade da imagem de AnyConnect

Recursos não suportados

- IKEv2, IKEv1
- Failover stateful
- Virtualização instantânea
- Configuração da imagem de AnyConnect pelo contexto
- WebLaunch
- Transferência do perfil do cliente
- DAP e CoA
- CSD/Hostscan
- Função de balanceamento de carga VPN
- Username--certificado e prefill-username
- Personalização/localização

Licenciar

- Licença do vértice de AnyConnect exigida
- Os fundamentos licenciam ignorado/não reservado

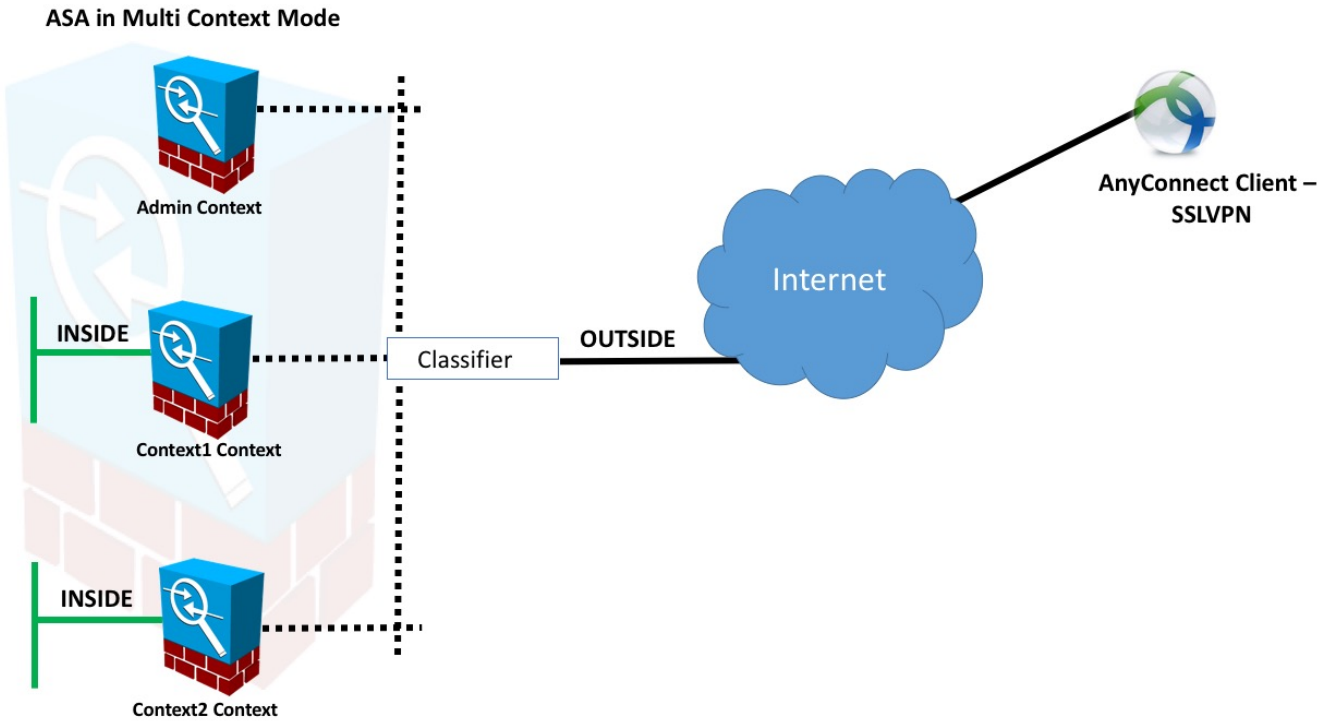
- Configurability para controlar o uso máximo da licença pelo contexto
- Configurability para permitir a licença que estoura pelo contexto

Configurar

Esta seção descreve como configurar Cisco ASA como um server local de CA.

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede



> **Nota:** Os contextos múltiplos neste exemplo compartilham de uma relação (FORA), a seguir o classificador usa os endereços originais da relação (auto ou) MAC manual para enviar pacotes. Para mais detalhes como a ferramenta de segurança classifica em pacotes no contexto múltiplo consulte como o ASA classifica pacotes

Configurações

Contexto do sistema

Etapa 1. Configuração de failover.

```
 !! Active Firewall

failover
failover lan unit primary
failover lan interface LAN_FAIL GigabitEthernet0/3
```

```
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2

 !! Secondary Firewall

failover
failover lan unit secondary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2
```

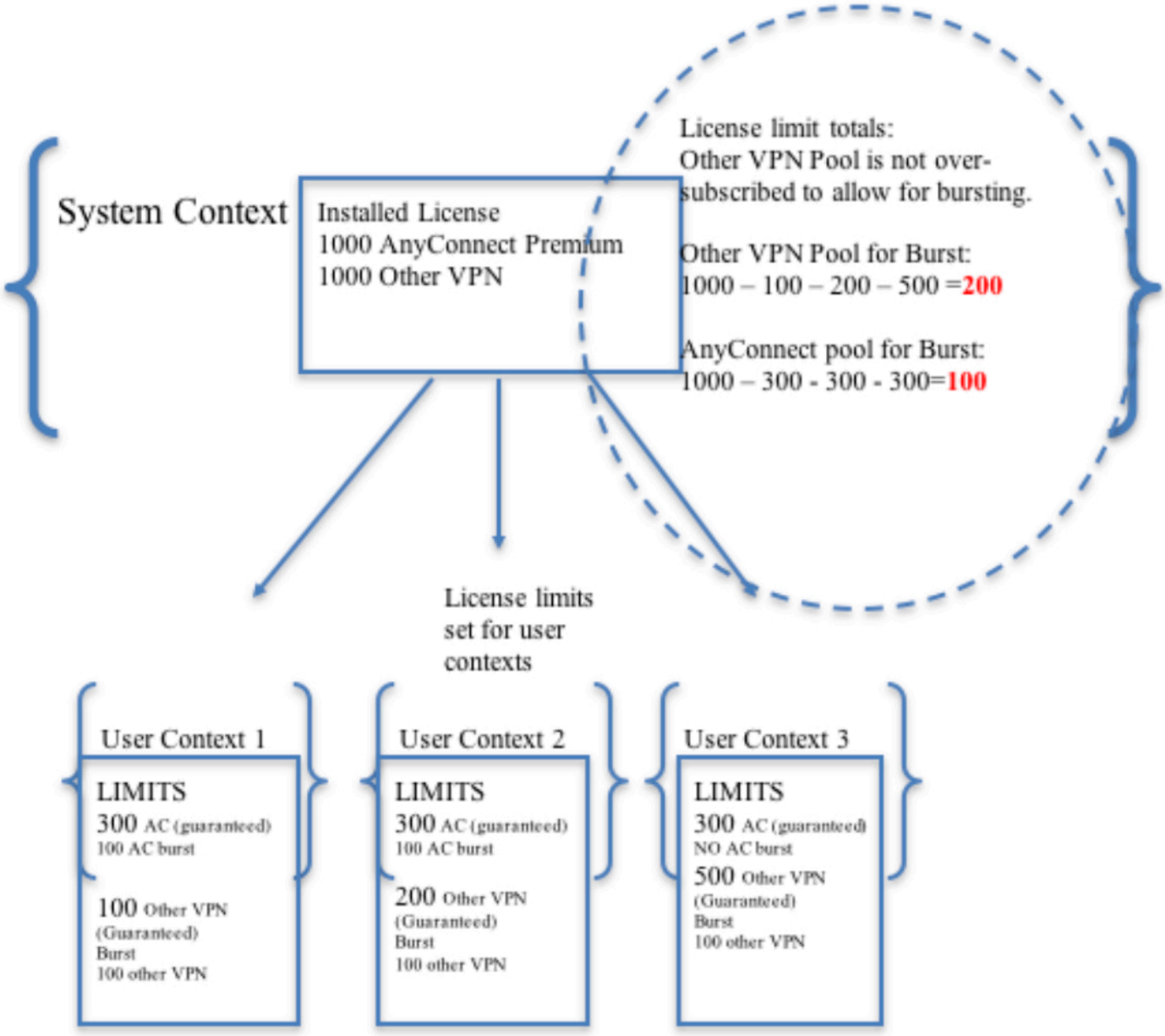
Etapa 2. Atribua VPN Resouce.

Configurado através de configuração existente da classe…. As licenças são permitidas pelo número de licenças ou pelos % do total pelo contexto

Tipos de recurso novos introduzidos para MC RAVPN:

- VPN AnyConnect: Garantido a um contexto e não pode ser oversubscribed
- Explosão AnyConnect VPN: Permita a contexto licenças extra além do limite garantido. O pool da explosão consiste em todas as licenças não garantidas a um contexto e é permitido a um contexto de estouro em uma primeiro a chegar primeiro a ser servido base

Modelo do abastecimento da licença VPN:



Nota: ASA5585 oferece 10,000 sessões do usuário máximas de Cisco AnyConnect e neste Cisco AnyConnect do exemplo 4000 a sessão do usuário é atribuída pelo contexto.

```
class resource02
 limit-resource VPN AnyConnect  4000
 limit-resource VPN Burst AnyConnect  2000

class resource01
 limit-resource VPN AnyConnect 4 000
 limit-resource VPN Burst AnyConnect  2000
```

Etapa 3. Configurar contextos e atribua recursos.

Nota: Neste exemplo GigabitEthernet0/0 é compartilhado entre todo o contexto.

```
admin-context admin
context admin
  allocate-interface GigabitEthernet0/0
  config-url disk0:/admin

context context1
  member resource01
```

```
  allocate-interfaceGigabitEthernet0/0
  allocate-interface GigabitEthernet0/1
  config-url disk0:/context1
  join-failover-group 1

context context2
  member resource02
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/2
  config-url disk0:/context2
  join-failover-group 2
```

Etapa 4. Instale a licença do vértice no Firewall.

Ativando ou desativando chaves de ativação

Contexto Admin

Etapa 1. Instale o pacote do cliente de AnyConnect.

> **Nota:** 1. O armazenamento instantâneo não é virtualizado e é somente acessível do contexto do sistema.
> 2. Copie arquivos ao flash na imagem de AnyConnect do contexto do sistema isto é.
> 3. A imagem de AnyConnect é uma configuração compartilhada.
> 4. Configurado no contexto admin somente. Não disponível em outros contextos.
> 5. Todos os contextos referem automaticamente esta configuração global da imagem de AnyConnect.

```
webvpn
 anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
 anyconnect enable
```

Contexto feito sob encomenda 1

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 10.106.44.38  255.255.255.0 standby 10.106.44.39

!! Enable WebVPN on respective interfaces

webvpn
 enable OUTSIDE
 anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
 banner value "Welcome to Context1 SSLVPN"
 wins-server none
```

```
 dns-server value 192.168.20.10
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
 address-pool mypool
 default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
 group-alias MC_RAVPN_1 enable
 group-url https://10.106.44.38/context1  enable
```

Contexto feito sob encomenda 2

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 10.106.44.36  255.255.255.0 standby 10.106.44.37

!! Enable WebVPN on respective interface

webvpn
 enable OUTSIDE
 anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
 banner value "Welcome to Context2 SSLVPN"
 wins-server none
 dns-server value 192.168.60.10
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com

tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
 address-pool mypool
 default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
 group-alias MC_RAVPN_2 enable
 group-url https://10.106.44.36/context2 enable
```

Verificar

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

> Nota: A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do

emissor de comando de execução.

Verifique se a licença do vértice é instalada

O ASA não reconhece especificamente uma licença do vértice de AnyConnect mas reforça as características da licença de uma licença do vértice que incluem:

- Prêmio de AnyConnect licenciado ao limite da plataforma
- AnyConnect para o móbil
- AnyConnect para o telefone de Cisco VPN
- Avaliação avançada do valor-limite

Verifique se o pacote de AnyConnect é instalado no contexto Admin e está disponível em contextos feitos sob encomenda

```
 !! AnyConnect package is installed in Admin Context

ciscoasa/pri/ admin/act# show run webvpn
webvpn
 anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
 anyconnect enable

ciscoasa/pri/admin/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,1,10010
  Hostscan Version 3.1.10010
  Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed

!! AnyConnect package is available in context1
ciscoasa/pri/admin/act# changeto context context1

ciscoasa/pri/context1/act# show run webvpn
webvpn
 enable OUTSIDE
 anyconnect enable
 tunnel-group-list enable

ciscoasa/pri/context1/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,1,10010
  Hostscan Version 3.1.10010
  Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed
```

Verifique se os usuários podem conectar através de AnyConnect em contextos feitos sob encomenda

Dica: Para o melhor relógio do indicador abaixo dos vídeos na tela cheia.

```
 !! One Active Connection on Context1
```

```
ciscoasa/pri/context1/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 5
Assigned IP  : 192.168.1.1            Public IP    : 10.142.168.102
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium, AnyConnect for Mobile
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 3186                   Bytes Rx     : 426
Group Policy : GroupPolicy_MC_RAVPN_1 Tunnel Group : MC_RAVPN_1
Login Time   : 15:33:25 UTC Thu Dec 3 2015
Duration     : 0h:00m:05s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6a2c2600005000566060c5
Security Grp : none

!! Changing Context to Context2

ciscoasa/pri/context1/act# changeto context context2

!! One Active Connection on Context2

ciscoasa/pri/context2/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 1
Assigned IP  : 192.168.51.1           Public IP    : 10.142.168.94
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10550                  Bytes Rx     : 1836
Group Policy : GroupPolicy_MC_RAVPN_2 Tunnel Group : MC_RAVPN_2
Login Time   : 15:34:16 UTC Thu Dec 3 2015
Duration     : 0h:00m:17s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6a2c2400001000566060f8
Security Grp : none

!! Changing Context to System

ciscoasa/pri/context2/act# changeto system

!! Notice total number of connections are two (for the device)

ciscoasa/pri/act# show vpn-sessiondb license-summary
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
                                   Status : Capacity : Installed :  Limit
                                 ----------------------------------------
AnyConnect Premium               :  ENABLED :    10000 :     10000 :   NONE
Other VPN (Available by Default) :  ENABLED :    10000 :     10000 :   NONE
AnyConnect for Mobile            :  ENABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment     :  ENABLED(Requires Premium)
AnyConnect for Cisco VPN Phone   :  ENABLED
VPN-3DES-AES                     :  ENABLED
VPN-DES                          :  ENABLED
----------------------------------------------------------------------------
```

```
-------------------------------------------------------------------------
VPN Licenses Usage Summary
-------------------------------------------------------------------------
                        Local : Shared :   All  :   Peak :  Eff.  :
                       In Use : In Use : In Use : In Use :  Limit : Usage
                      ---------------------------------------------------
AnyConnect Premium     :      2 :      0 :       2 :      2 :  10000 :    0%
 AnyConnect Client    :                 :      2 :      2          :    0%
   AnyConnect Mobile  :                 :      2 :      2          :    0%
Other VPN             :                 :      0 :      0 :  10000 :    0%
 Site-to-Site VPN     :                 :      0 :      0          :    0%
-------------------------------------------------------------------------

!! Notice the resource usage per Context

ciscoasa/pri/act# show resource usage all resource VPN AnyConnect
Resource                 Current        Peak      Limit        Denied Context
AnyConnect                     1           1       4000             0 context1
AnyConnect                     1           1       4000             0 context2
```

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Pesquisando defeitos AnyConnect

> **Dica:** Caso que o ASA não tem a licença do vértice instalada, a sessão de AnyConnect estaria terminada com Syslog abaixo:
>
> %ASA-6-725002: O dispositivo terminou a saudação de SSL com cliente OUTSIDE:10.142.168.86/51577 a 10.106.44.38/443 para a sessão TLSv1
> %ASA-6-113012: Autenticação de usuário AAA bem sucedida: base de dados local: user = Cisco
> %ASA-6-113009: O AAA recuperou a política do grupo padrão (GroupPolicy_MC_RAVPN_1) para o user = Cisco
> %ASA-6-113008: O estado de transação AAA ACEITA: user = Cisco
> %ASA-3-716057: Sessão IP <10.142.168.86> do usuário do grupo terminada, nenhuma licença do vértice de AnyConnect disponível
> %ASA-4-113038: IP <10.142.168.86> do usuário do grupo incapaz de criar a sessão do pai de AnyConnect.

Referências

Notas de versão: 9.5(2)

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Guia de Troubleshooting do cliente VPN de AnyConnect - Problemas comuns
- Controlando, monitorando, e pesquisando defeitos sessões de AnyConnect
- Suporte Técnico e Documentação - Cisco Systems