Balanceamento de carga remoto do cliente VPN no exemplo de configuração ASA 5500

Índice

Introdução

O balanceamento de carga é a capacidade de ter Cisco VPN Clients compartilhados entre várias unidades de Adaptive Security Appliance (ASA) sem a intervenção do usuário. A função de balanceamento de carga garante que o endereço IP público esteja altamente disponível aos usuários. Por exemplo, se o Cisco ASA que mantém o endereço IP público falha, um outro ASA no cluster assume o endereço IP público.

Pré-requisitos

Requisitos

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

- Você tem endereços IP atribuídos em seus ASA e configurou o gateway padrão.
- O IPsec é configurado nos ASA para os usuários de cliente VPN.
- Os usuários VPN podem conectar individualmente a todos os ASA com o uso de seu endereço IP público atribuído.

Clientes elegíveis

O Balanceamento de carga é eficaz somente nas sessões remotas iniciadas com estes clientes:

- Cisco VPN Client (3.0 da liberação ou mais tarde)
- Cisco VPN 3002 Hardware Client (liberação 3.5 ou mais atrasado)
- CiscoASA 5505 ao atuar como um cliente VPN fácil

Todos clientes restantes, incluindo conexões de LAN para LAN, podem conectar a uma ferramenta de segurança em que o Balanceamento de carga é permitido, mas não podem participar no Balanceamento de carga.

Componentes Utilizados

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

- Software Release 4.6 e Mais Recente do cliente VPN
- Software Release 7.0.1 e Mais Recente de Cisco ASA**Nota:** Estende o apoio do Balanceamento de carga a ASA 5510 e o ASA modela mais tarde de 5520 que têm uma Segurança mais a licença com 8.0(2) a versão.

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Restrições

- O endereço IP do cluster virtual de VPN, a porta do Protocolo de datagrama de usuário (UDP) e o segredo compartilhado devem ser idênticos em todos os dispositivos no cluster virtual.
- Todos os dispositivos no cluster virtual devem estar no mesmo sub-redes IP exterior e interno.

Configuração

Atribuição de endereço IP:

Assegure-se de que os endereços IP de Um ou Mais Servidores Cisco ICM NT estejam configurados na parte externa e nas interfaces internas e você possa obter ao Internet de seu

ASA.

Nota: Assegure-se de que o ISAKMP esteja permitido em ambos a interface interna e externa. Selecione a **configuração > as características > o VPN > o IKE > os parâmetros globais** a fim verificar isto.

Configuração de cluster

Este procedimento mostra como usar o Cisco Adaptive Security Device Manager (ASDM) para configurar o Balanceamento de carga.

Nota: Muitos dos parâmetros neste exemplo têm valores padrão.

1. Selecione a **configuração > as características > o VPN > o Balanceamento de carga**, e a verificação **participa no conjunto do Balanceamento de carga** para permitir o Balanceamento de carga VPN.
2. Termine estas etapas para configurar os parâmetros para todos os ASA que participam no conjunto na caixa de grupo da configuração de grânulos VPN:Datilografe o endereço IP de Um ou Mais Servidores Cisco ICM NT do conjunto na caixa de texto do endereço IP de Um ou Mais Servidores Cisco ICM NT do conjunto.O clique **permite a criptografia IPSec**.Datilografe a chave de criptografia na caixa de texto do segredo compartilhado de IPSec e datilografe-a outra vez na caixa de texto do segredo da verificação.
3. Configurar as opções na caixa de grupo de configuração do servidor de VPN:Selecione uma relação que aceite as conexões de VPN entrantes na lista pública.Selecione uma relação que seja a interface confidencial na lista privada.(*Opcional*) mude a prioridade que o ASA tem no conjunto na caixa de texto da prioridade.Datilografe um endereço IP de Um ou Mais Servidores Cisco ICM NT para o endereço IP atribuído do Network Address Translation (NAT) se este dispositivo é atrás de um Firewall que use o NAT.
4. Repita as etapas em todos os ASA de participação no grupo.

O exemplo nesta seção usa estes comandos CLI configurar o Balanceamento de carga:

```
VPN-ASA2(config)#vpn load-balancing VPN-ASA2(config-load-balancing)#priority 10 VPN-ASA2(config-load-balancing)#cluster key cisco123 VPN-ASA2(config-load-balancing)#cluster ip address 172.16.172.54 VPN-ASA2(config-load-balancing)#cluster encryption VPN-ASA2(config-load-balancing)#participate
```

Monitoramento

Selecione a **monitoração > as características > o VPN > as estatísticas de VPN > as cargas do conjunto** para monitorar a característica do Balanceamento de carga no 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.

- **mostre a função de balanceamento de carga do vpn** — Verifica a característica do Balanceamento de carga VPN.`Status: enabled`

```
Role: Backup
Failover: n/a
Encryption: enabled
Cluster IP: 172.16.172.54
Peers: 1

Public IP Role Pri Model Load (%) Sessions
-----------------------------------------------------------
* 172.16.172.53 Backup 5 ASA-5520 0 1
172.16.172.52 Master 4 ASA-5520 n/a n/a
```

Troubleshooting

Use esta seção para resolver problemas de configuração.

Comandos para Troubleshooting

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.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **debugar o vpnlb 250** — Usado para pesquisar defeitos a característica do Balanceamento de carga VPN.`VPN-ASA2#`

```
VPN-ASA2# 5718045: Created peer[172.16.172.54]
5718012: Sent HELLO request to [172.16.172.54]
5718016: Received HELLO response from [172.16.172.54]
7718046: Create group policy [vpnlb-grp-pol]
7718049: Created secure tunnel to peer[192.168.0.11]
5718073: Becoming slave of Load Balancing in context 0.
5718018: Send KEEPALIVE request failure to [192.168.0.11]
5718018: Send KEEPALIVE request failure to [192.168.0.11]
5718018: Send KEEPALIVE request failure to [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718035: Received TOPOLOGY indicator from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
```

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems