Configurando o modo NAT Transparent para IPSec no VPN 3000 Concentrator

Contents

Introduction

A Tradução de Endereço de Rede (NAT) foi desenvolvida para tratar do problema da versão 4 do Protocolo de Internet (IPV4) que estava ficando sem espaço de endereços. Hoje, os usuários domésticos e as pequenas redes de escritórios usam NAT como uma alternativa à aquisição de endereços registrados. As corporações implantam NAT, sozinha ou com um firewall, para proteger seus recursos internos.

Muitos para um, a solução NAT mais comumente implementada, mapeia vários endereços privados para um único endereço roteável (público); isso também é conhecido como Port Address Translation (PAT). A associação é implementada no nível da porta. A solução PAT cria um problema para o tráfego IPSec que não usa nenhuma porta.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco VPN 3000 Concentrator
- Cisco VPN 3000 Client versão 2.1.3 e posterior
- Cisco VPN 3000 Client and Concentrator versão 3.6.1 e posterior para NAT-T

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Encapsulando o payload de segurança

O Protocolo 50 (Encapsulating Security Payload [ESP]) manipula os pacotes criptografados/encapsulados de IPSec. A maioria dos dispositivos PAT não funciona com o ESP, pois foram programados para funcionar somente com o Transmission Control Protocol (TCP), User Datagram Protocol (UDP) e Internet Control Message Protocol (ICMP). Além disso, os dispositivos PAT não podem mapear vários índices de parâmetros de segurança (SPIs). O modo transparente de NAT no VPN 3000 Client resolve esse problema encapsulando o ESP no UDP e enviando-o para uma porta negociada. O nome do atributo a ser ativado no VPN 3000 Concentrator é IPSec por NAT.

Um novo protocolo NAT-T que é um padrão IETF (ainda no estágio de RASCUNHO a partir da redação deste artigo) também encapsula pacotes IPSec no UDP, mas funciona na porta 4500. Essa porta não é configurável.

Como funciona o modo transparente da NAT?

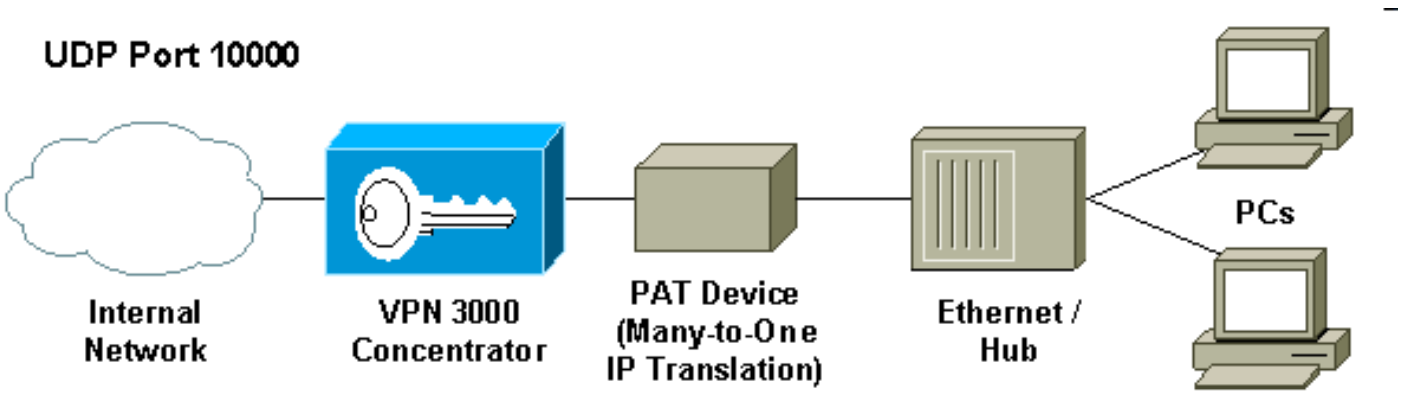
A ativação do modo transparente de IPSec no VPN Concentrator cria regras de filtro não visíveis e as aplica ao filtro público. O número de porta configurado é então passado para o VPN Client de forma transparente quando o VPN Client se conecta. No lado de entrada, o tráfego de entrada UDP dessa porta passa diretamente para o IPSec para processamento. O tráfego é descriptografado e desencapsulado e, em seguida, roteado normalmente. No lado de saída, o IPSec criptografa, encapsula e aplica um cabeçalho UDP (se configurado). As regras de filtro de tempo de execução são desativadas e eliminadas do filtro apropriado em três condições: quando o IPSec sobre UDP é desabilitado para um grupo, quando o grupo é excluído ou quando o último IPSec sobre UDP SA ativo nessa porta é excluído. Keepalives são enviados para impedir que um dispositivo NAT feche o mapeamento de porta devido à inatividade.

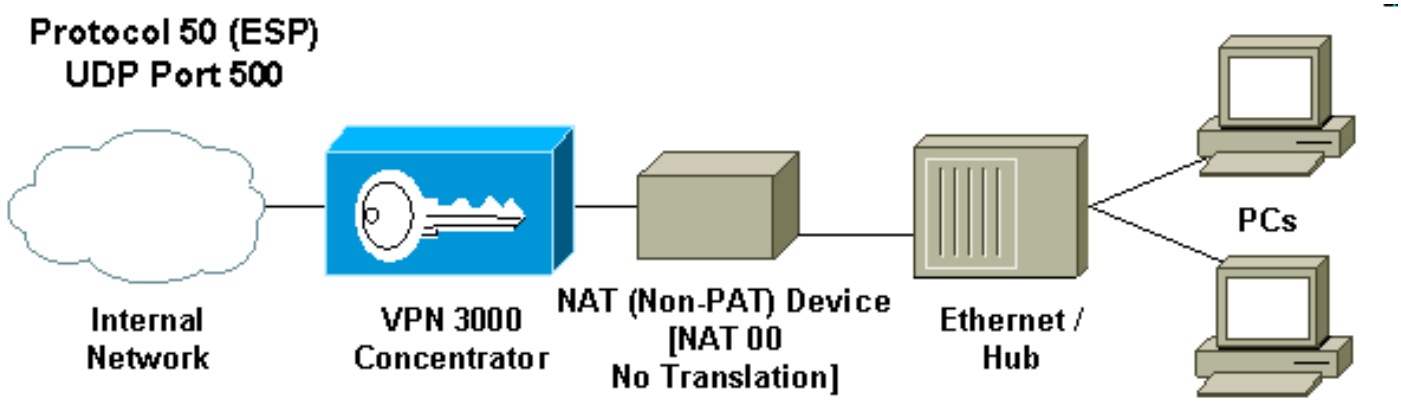
Se o IPSec sobre NAT-T estiver ativado no VPN Concentrator, o VPN Concentrator/VPN Client usará o modo NAT-T de encapsulamento UDP. O NAT-T funciona detectando automaticamente qualquer dispositivo NAT entre o VPN Client e o VPN Concentrator durante a negociação de IKE. Você deve garantir que a porta UDP 4500 não seja bloqueada entre o VPN Concentrator/VPN Client para que o NAT-T funcione. Além disso, se estiver usando uma configuração anterior de IPSec/UDP que já esteja usando essa porta, você deverá reconfigurar a configuração anterior de IPSec/UDP para usar uma porta UDP diferente. Como o NAT-T é um rascunho IETF, ele ajuda ao usar dispositivos de vários fornecedores se o outro fornecedor implementar esse padrão.

O NAT-T funciona com conexões de VPN Client e conexões LAN a LAN, diferentemente do IPSec sobre UDP/TCP. Além disso, os roteadores Cisco IOS® e os dispositivos de firewall PIX suportam NAT-T.

Você não precisa que o IPSec sobre UDP seja habilitado para que o NAT-T funcione.

Configurar o modo transparente de NAT





Use o procedimento a seguir para configurar o modo transparente de NAT no VPN Concentrator.

Observação: o IPSec sobre UDP é configurado por grupo, enquanto o IPSec sobre TCP/NAT-T é configurado globalmente.

1. Configurar IPSec sobre UDP:No VPN Concentrator, selecione **Configuration > User Management > Groups** (**Configuração > Gerenciamento de usuários > Grupos**).Para adicionar um grupo, selecione **Adicionar**. Para modificar um grupo existente, selecione-o e clique em **Modificar**.Clique na guia IPSec, marque **IPSec por NAT** e configure o **IPSec por meio da porta NAT UDP**. A porta padrão para IPSec através de NAT é 10000 (origem e destino), mas essa configuração pode ser alterada.
2. Configurar IPSec sobre NAT-T e/ou IPSec sobre TCP:No VPN Concentrator, selecione Configuration > **System > Tunneling Protocols > IPSec > NAT Transparency**.Marque a caixa de seleção **IPSec sobre NAT-T e/ou TCP**.

Se tudo estiver ativado, use esta precedência:

1. IPSec sobre TCP.
2. IPSec sobre NAT-T.
3. IPSec sobre UDP.

Configuração do Cisco VPN Client para usar transparência de NAT

Para usar IPSec sobre UDP ou NAT-T, você precisa habilitar IPSec sobre UDP no Cisco VPN Client 3.6 e posterior. A porta UDP é atribuída pelo VPN Concentrator no caso de IPSec sobre UDP, enquanto para NAT-T é fixada à porta UDP 4500.

Para usar IPSec sobre TCP, você precisa ativá-lo no VPN Client e configurar a porta que deve ser usada manualmente.

Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems