Configurando o modo NAT Transparent para IPSec no VPN 3000 Concentrator

Índice

Introdução

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.

Muito-a-um, a solução o mais geralmente executada NAT, traça diversos endereços privados a um único endereço do roteável (público); isto é sabido igualmente como a tradução de endereço de porta (PAT). A associação é executada a nível da porta. A solução da PANCADINHA cria um problema para o tráfego de IPSec que não usa nenhuma portas.

Pré-requisitos

Requisitos

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
- Liberação de Cisco VPN 3000 Client 2.1.3 e mais atrasado
- Cisco VPN 3000 Client e versão do concentrador 3.6.1 e mais atrasado para o NAT-T

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

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Encapsulando o payload de segurança

Os 50 pés do protocolo ([ESP] do Encapsulating Security Payload) seguram cifrado/pacotes encapsulado de IPsec. A maioria de dispositivos da PANCADINHA não funcionam com ESP desde que foram programados para trabalhar somente com Transmission Control Protocol (TCP), User Datagram Protocol (UDP), e Internet Control Message Protocol (ICMP). Além, os dispositivos da PANCADINHA são incapazes de traçar os deslocamentos predeterminados múltiplos do parâmetro de segurança (SPI). O modo transparente NAT no VPN 3000 Client resolve este problema encapsulando o ESP dentro do UDP e enviando o a uma porta negociada. O nome do atributo a ativar no VPN 3000 concentrator é IPsec com o NAT.

Um protocolo novo NAT-T que seja um padrão de IETF (ainda na fase do ESBOÇO até à data da escrita este artigo) igualmente encapsular-lo pacotes de IPsec no UDP, mas trabalha na porta 4500. Essa porta não é configurável.

Como funciona o modo transparente da NAT?

O modo transparente de ativação do IPsec no concentrador VPN cria regras de filtro não visível e aplica-as ao filtro público. O número de porta configurada está passado então ao cliente VPN transparentemente quando o cliente VPN conecta. No lado de entrada, o tráfego de entrada UDP dessa porta passa diretamente ao IPsec para processar. O tráfego é decifrado e descapsulado, e distribuído então normalmente. No lado externo, o IPsec cifra, encapsula e aplica então um cabeçalho de UDP (se configurado assim). As regras de filtro runtime são desativadas e suprimidas do filtro apropriado sob três circunstâncias: quando o IPsec sobre o UDP estiver desabilitado para um grupo, quando o grupo estiver suprimido, ou quando o último IPSec ativo sobre UDP SA nessa porta estiver suprimido. O Keepalives é enviado para impedir que um dispositivo NAT feche o mapeamento de porta devido à inatividade.

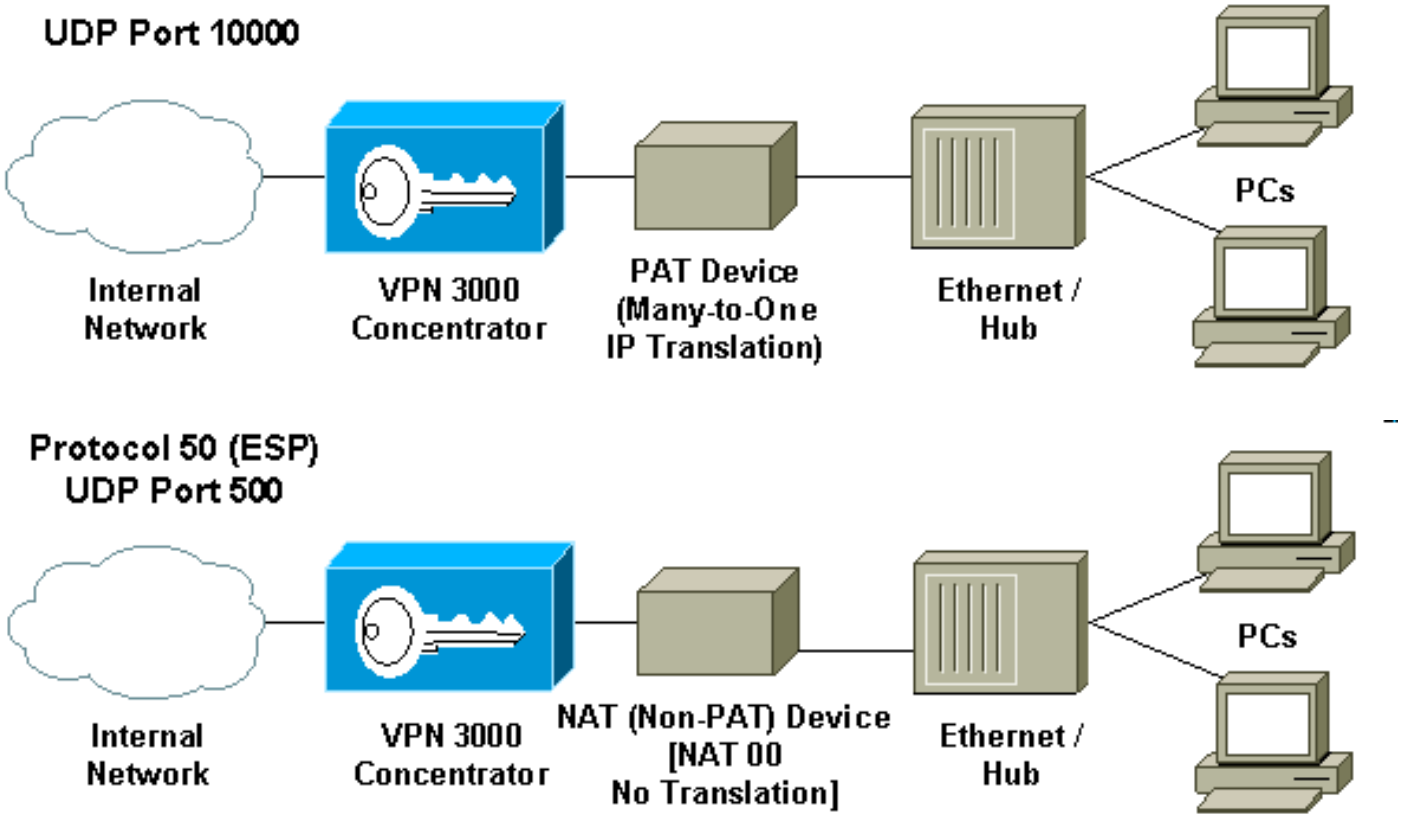
Se o IPsec sobre o NAT-T é permitido no concentrador VPN, a seguir o cliente VPN Concentrator/VPN usa o modo de encapsulamento de UDP NAT-T. O NAT-T trabalha auto-detectando todo o dispositivo NAT entre o cliente VPN e o concentrador VPN durante a negociação de IKE. Você deve assegurar-se de que a porta 4500 UDP não esteja obstruída entre o cliente VPN Concentrator/VPN para que o NAT-T trabalhe. Também, se você está usando uma configuração precedente IPSec/UDP que já esteja usando essa porta, você deve reconfigurar essa configuração mais adiantada IPSec/UDP para usar uma porta diferente UDP. Desde que o NAT-T é um esboço de IETF, ajuda ao usar dispositivos multivendor se o outro fornecedor executa este padrão.

O NAT-T trabalha com as conexões de cliente de VPN e o IPsec desigual das conexões de LAN para LAN sobre o UDP/TCP. Também, o Roteadores de Cisco IOS® e os dispositivos do PIX

Firewall apoiam o NAT-T.

Você não precisa o IPsec sobre o UDP de ser permitido de ter o funcionamento NAT-T.

Configurar o modo transparente NAT



Use o seguinte procedimento para configurar o modo transparente NAT no concentrador VPN.

Note: O IPsec sobre o UDP está configurado na pela base do grupo, quando o IPsec sobre TCP/NAT-T for configurado globalmente.

1. Configurar o IPsec sobre o UDP:No concentrador VPN, selecione o **configuration > user management > os grupos**.Para adicionar um grupo, seleto **adicionar**. Para alterar um grupo existente, para selecionar o e o clique **altera**.Clique a aba do IPsec, verifique o **IPsec com o NAT** e configurar o **IPsec através da porta NAT UDP**. A porta padrão para o IPsec com o NAT é 10000 (fonte e destino), mas este ajuste pode ser mudado.
2. Configurar o IPsec sobre o NAT-T e/ou o IPsec sobre o TCP:No concentrador VPN selecione o **Configuration > System** > Tunneling Protocols > **IPsec > transparência de NAT**.Verifique o **IPsec sobre o NAT-T e/ou a caixa de verificação de TCP**.

Se tudo é permitido, use esta precedência:

1. IPsec sobre o TCP.
2. IPsec sobre o NAT-T.
3. IPsec sobre o UDP.

Configuração de Cisco VPN Client para usar a transparência de NAT

Para usar o IPsec sobre o UDP ou o NAT-T que você precisa de permitir o IPsec sobre o UDP no 3.6 e mais recente do Cisco VPN Client. A porta UDP está atribuída pelo concentrador VPN em caso do IPsec sobre o UDP, quando para o NAT-T for fixada à porta 4500 UDP.

Para usar o IPsec sobre o TCP, você precisa de permiti-lo no cliente VPN e de 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