Configurazione della modalità trasparente NAT per IPSec sul concentratore VPN 3000

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Payload di sicurezza incapsulante
Come funziona la modalità trasparente NAT?
Configura modalità trasparente NAT
Configurazione di Cisco VPN Client per utilizzare la trasparenza NAT
Informazioni correlate

Introduzione

Network Address Translation (NAT) è stato sviluppato per risolvere il problema relativo all'esaurimento dello spazio degli indirizzi del protocollo IP versione 4 (IPV4). Oggi, gli utenti privati e le piccole reti aziendali usano NAT come alternativa all'acquisto di indirizzi registrati. Le aziende implementano NAT da sole o con un firewall per proteggere le risorse interne.

Many-to-one, la soluzione NAT più comunemente implementata, mappa diversi indirizzi privati su un singolo indirizzo (pubblico) instradabile; questo processo è noto anche come PAT (Port Address Translation). L'associazione viene implementata a livello di porta. La soluzione PAT crea un problema per il traffico IPSec che non utilizza alcuna porta.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco VPN 3000 Concentrator
- Cisco VPN 3000 Client release 2.1.3 e successive
- Cisco VPN 3000 Client e concentrator release 3.6.1 e successive per NAT-T

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Payload di sicurezza incapsulante

Il protocollo 50 (Encapsulating Security Payload [ESP]) gestisce i pacchetti crittografati/incapsulati di IPSec. La maggior parte dei dispositivi PAT non funziona con ESP in quanto sono stati programmati per funzionare solo con il protocollo TCP (Transmission Control Protocol), UDP (User Datagram Protocol) e ICMP (Internet Control Message Protocol). Inoltre, i dispositivi PAT non sono in grado di mappare più indici dei parametri di sicurezza (SPI). La modalità trasparente NAT nel client VPN 3000 risolve questo problema incapsulando ESP in UDP e inviandolo a una porta negoziata. Il nome dell'attributo da attivare sul concentratore VPN 3000 è IPSec tramite NAT.

Un nuovo protocollo NAT-T che è uno standard IETF (ancora in fase DRAFT al momento della stesura di questo articolo) incapsula anche i pacchetti IPSec in UDP, ma funziona sulla porta 4500. Porta non configurabile.

Come funziona la modalità trasparente NAT?

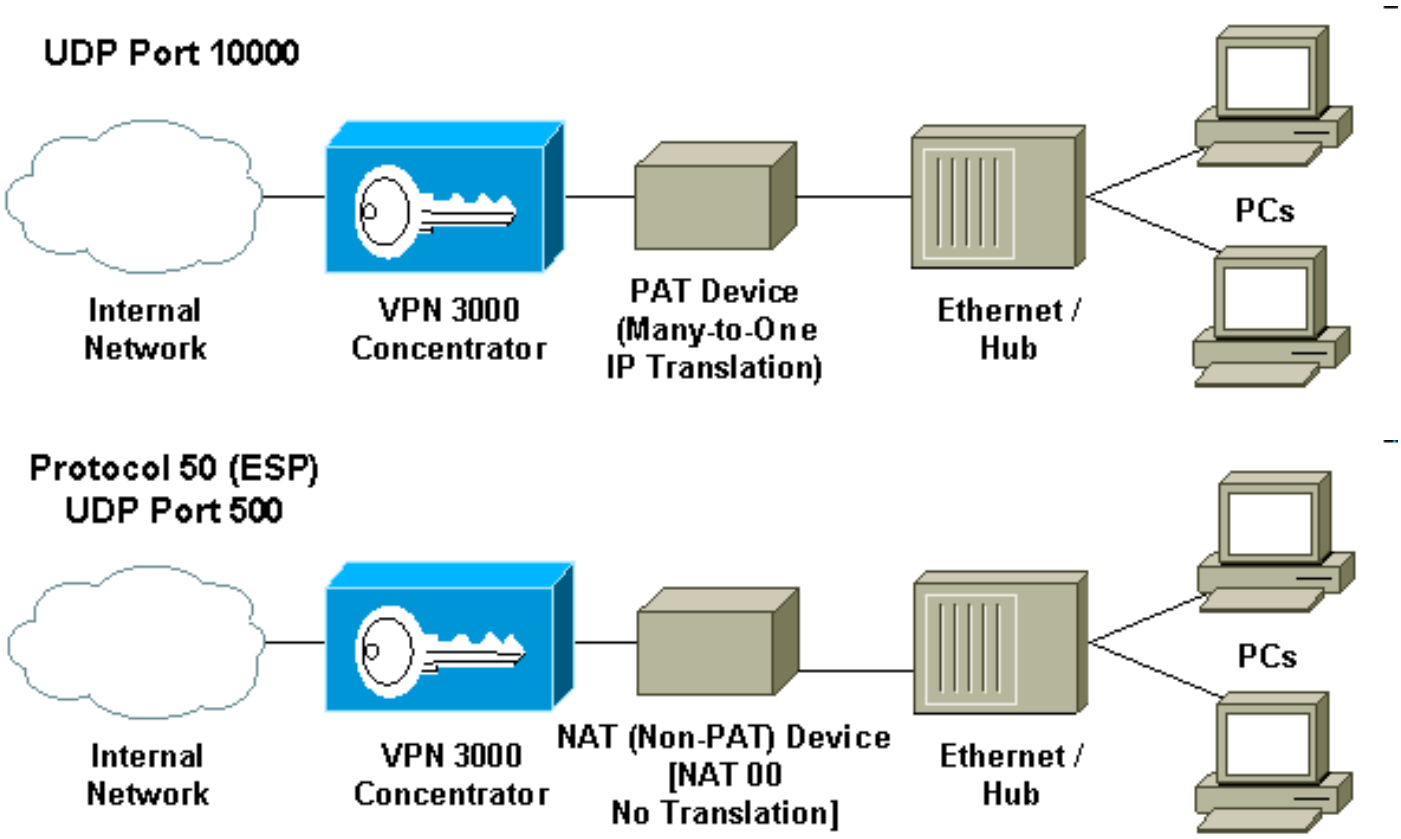
L'attivazione della modalità trasparente IPSec in Concentrator VPN crea regole di filtro non visibili e le applica al filtro pubblico. Il numero di porta configurato viene quindi passato al client VPN in modo trasparente quando il client VPN si connette. Sul lato in entrata, il traffico UDP in entrata proveniente da tale porta passa direttamente a IPSec per l'elaborazione. Il traffico viene decapsulato e decapsulato, quindi indirizzato normalmente. Sul lato uscita, IPSec esegue la crittografia, incapsula e quindi applica un'intestazione UDP (se configurata in questo modo). Le regole di filtro di runtime vengono disattivate ed eliminate dal filtro appropriato in tre condizioni: quando IPSec over UDP è disabilitato per un gruppo, quando il gruppo viene eliminato o quando viene eliminato l'ultimo IPSec over UDP SA attivo su tale porta. I pacchetti keepalive vengono inviati per impedire al dispositivo NAT di chiudere il mapping delle porte per inattività.

Se nel concentratore VPN è abilitato IPSec over NAT-T, il client VPN utilizza la modalità NAT-T di incapsulamento UDP. NAT-T funziona rilevando automaticamente qualsiasi dispositivo NAT tra il client VPN e il concentratore VPN durante la negoziazione IKE. Affinché NAT-T funzioni, è necessario verificare che la porta UDP 4500 non sia bloccata tra il client VPN Concentrator/VPN. Inoltre, se si utilizza una configurazione IPSec/UDP precedente che utilizza già tale porta, è necessario riconfigurare la configurazione IPSec/UDP precedente in modo che utilizzi una porta UDP diversa. Poiché NAT-T è una bozza IETF, se l'altro fornitore implementa questo standard è di aiuto nell'utilizzo di dispositivi multifornitore.

NAT-T funziona sia con le connessioni client VPN che con le connessioni LAN a LAN, a differenza di IPSec su UDP/TCP. Inoltre, i router Cisco IOS® e i dispositivi firewall PIX supportano NAT-T.

Per il funzionamento di NAT-T non è necessario che IPSec su UDP sia abilitato.

Configura modalità trasparente NAT



Utilizzare la procedura seguente per configurare la modalità trasparente NAT sul concentratore VPN.

Nota: IPSec over UDP è configurato per gruppo, mentre IPSec over TCP/NAT-T è configurato globalmente.

1. Configurare IPSec over UDP:Sul concentratore VPN, selezionare **Configurazione > Gestione utenti > Gruppi**.Per aggiungere un gruppo, selezionare **Aggiungi**. Per modificare un gruppo esistente, selezionarlo e fare clic su **Modifica**.Fare clic sulla scheda IPSec, selezionare **IPSec tramite NAT** e configurare **IPSec tramite porta UDP NAT**. La porta predefinita per IPSec tramite NAT è 10000 (origine e destinazione), ma è possibile modificare questa impostazione.
2. Configurare IPSec su NAT-T e/o IPSec su TCP:Sul concentratore VPN, selezionare Configuration > **System > Tunneling Protocols > IPSec > NAT Transparency**.Selezionare la casella di controllo **IPSec over NAT-T e/o TCP**.

Se sono abilitati tutti gli elementi, utilizzare la seguente precedenza:

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

Configurazione di Cisco VPN Client per utilizzare la trasparenza NAT

Per utilizzare IPSec su UDP o NAT-T, è necessario abilitare IPSec su UDP sul client VPN Cisco versione 3.6 e successive. La porta UDP è assegnata dal concentratore VPN in caso di IPSec su UDP, mentre per NAT-T è fissata alla porta UDP 4500.

Per utilizzare IPSec su TCP, è necessario attivarlo sul client VPN e configurare la porta da utilizzare manualmente.

Informazioni correlate

- Cisco VPN serie 3000 Concentrator Support Page
- Cisco VPN serie 3000 Client Support Page
- Pagina di supporto per IPSec
- Supporto tecnico – Cisco Systems