PIX/ASA 7.x e IOS: Frammentazione VPN

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi che possono verificarsi quando un pacchetto viene frammentato. Un esempio di problema di frammentazione è la capacità di eseguire il ping di una risorsa di rete, ma l'impossibilità di connettersi alla stessa risorsa con un'applicazione specifica, ad esempio un database o una posta elettronica.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

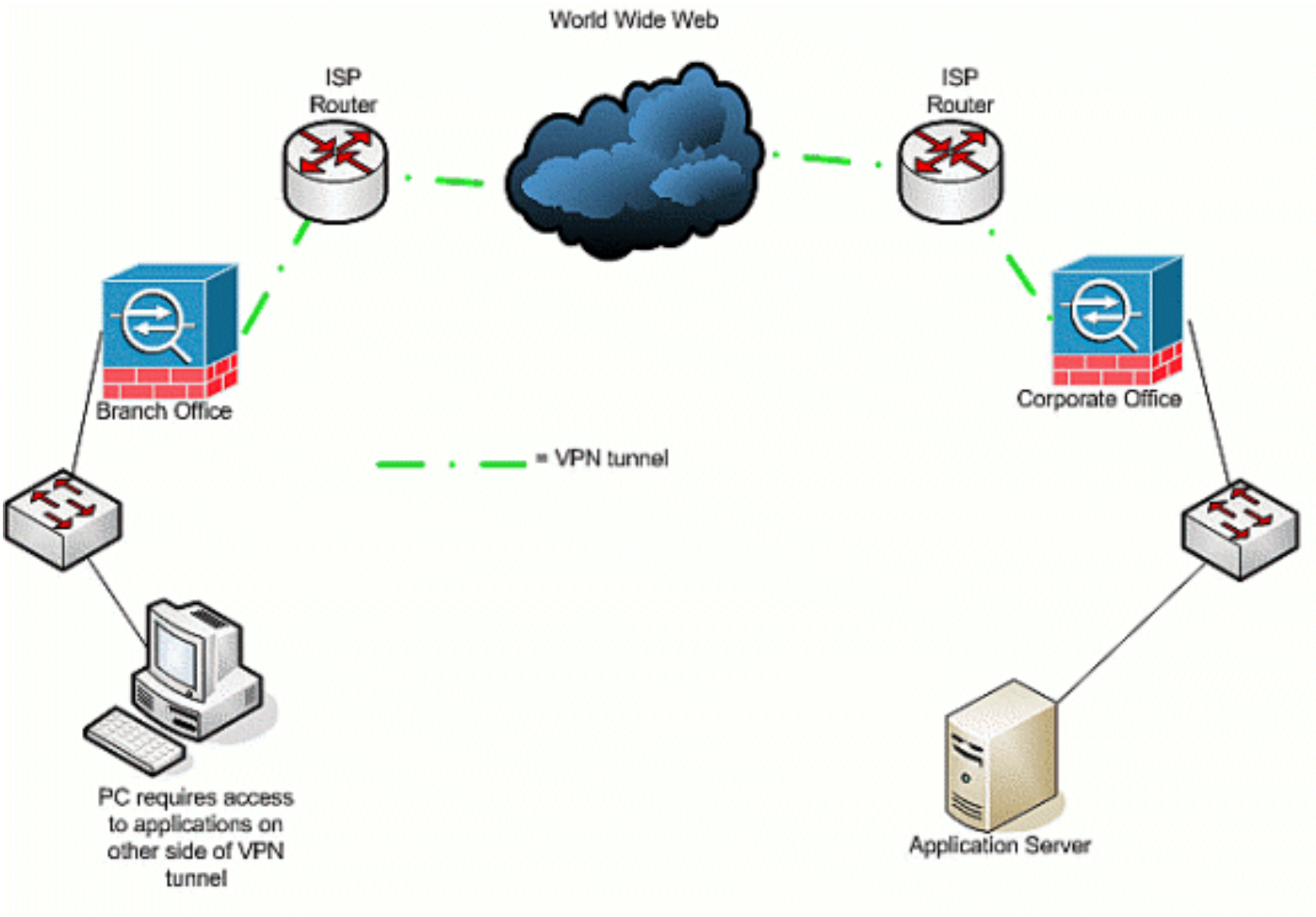
- Connettività tra peer VPN

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Prodotti correlati

Questa configurazione può essere utilizzata anche con le seguenti versioni hardware e software:

- Router IOS
- Dispositivi di sicurezza PIX/ASA

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

L'IP supporta una lunghezza massima di 65.536 byte per un pacchetto IP, ma la maggior parte dei protocolli del livello di collegamento dati supporta una lunghezza molto più piccola, chiamata MTU (Maximum Transmission Unit). In base all'MTU supportata, può essere necessario frammentare un pacchetto IP per trasmetterlo su un particolare tipo di supporto a livello di collegamento dati. Quindi, la destinazione deve ricomporre i frammenti nel pacchetto IP completo originale.

Protocol	Additional Bytes
ESP (encryption and hash)	56
AH	24+
GRE	24
NAT-T/IPsec over UDP (UDP part)	8
IPsec over TCP (TCP part)	20
L2TP	12
PPTP	48
Outer IP header in IPsec tunnel mode or PPTP/L2TP	20
PPPoE	8

Quando si utilizza una VPN per proteggere i dati tra due peer VPN, ai dati originali viene aggiunto un sovraccarico aggiuntivo che può richiedere la frammentazione. In questa tabella sono elencati i campi che potrebbero essere aggiunti ai dati protetti per supportare una connessione VPN. Si noti che possono essere necessari più protocolli, il che aumenta le dimensioni del pacchetto originale. Ad esempio, se si usa una connessione IPSEC DMVPN L2L tra due router Cisco, in cui è stato implementato un tunnel GRE, è necessario questo sovraccarico aggiuntivo: ESP, GRE e l'intestazione IP esterna. Se si dispone di una connessione client IPSec a un gateway VPN quando il traffico attraversa un dispositivo indirizzo, è necessario questo sovraccarico aggiuntivo per NAT-T (Network Address Translation- Traversal), nonché l'intestazione IP esterna per la connessione in modalità tunnel.

Problemi di frammentazione

Quando l'origine invia un pacchetto a una destinazione, inserisce un valore nel campo dei flag di controllo delle intestazioni IP che determina la frammentazione del pacchetto da parte dei dispositivi intermedi. Il flag di controllo è lungo tre bit, ma solo i primi due vengono utilizzati nella frammentazione. Se il secondo bit è impostato su 0, il pacchetto può essere frammentato; se è impostato su 1, il pacchetto non può essere frammentato. Il secondo bit è in genere denominato bit *non frammentare* (DF, Don't Fragment). Il terzo bit specifica quando si verifica la frammentazione, se il pacchetto frammentato è l'ultimo (impostato su 0) o se vi sono altri frammenti (impostato su 1) che costituiscono il pacchetto.

Quando è richiesta la frammentazione, le aree che possono creare problemi sono quattro:

- I due dispositivi che eseguono la frammentazione e il riassemblaggio richiedono un ulteriore sovraccarico nei cicli della CPU e nella memoria.
- Se un frammento viene scartato durante il percorso verso la destinazione, il pacchetto non può essere ricomposto e l'intero pacchetto deve essere frammentato e inviato di nuovo. Ciò crea ulteriori problemi di velocità effettiva, specialmente in situazioni in cui il traffico in questione è limitato dalla velocità e l'origine invia il traffico oltre il limite consentito.
- Il filtro dei pacchetti e i firewall con stato possono avere difficoltà nell'elaborare i frammenti. In

caso di frammentazione, il primo frammento contiene un'intestazione IP esterna, l'intestazione interna, ad esempio TCP, UDP, ESP e altri, e parte del payload. I frammenti successivi del pacchetto originale stipulano un'intestazione IP esterna e la continuazione del payload. Il problema di questo processo è che alcuni firewall devono visualizzare le informazioni dell'intestazione interna in ogni pacchetto per poter prendere decisioni intelligenti in materia di filtraggio; in caso contrario, possono eliminare inavvertitamente tutti i frammenti, ad eccezione del primo.

- L'origine nell'intestazione IP del pacchetto può impostare il terzo bit di controllo in modo che *non frammenti*, il che significa che se un dispositivo intermedio riceve il pacchetto e deve frammentarlo, il dispositivo intermedio non può frammentarlo. Al contrario, il dispositivo intermedio scarta il pacchetto.

Attività principale

Individua frammentazione

La maggior parte delle reti utilizza Ethernet, con un valore MTU predefinito di 1.500 byte, che è in genere utilizzato per i pacchetti IP. Per scoprire se la frammentazione si verifica o è necessaria, ma non può essere eseguita (il bit DF è impostato), avviare prima la sessione VPN. È quindi possibile utilizzare una di queste quattro procedure per individuare la frammentazione.

1. Eseguire il ping di una periferica situata all'altra estremità. In questo caso, si presume che il ping sia consentito attraverso il tunnel. Se l'operazione ha esito positivo, provare ad accedere a un'applicazione sullo stesso dispositivo; Se ad esempio un server di posta elettronica o di desktop remoto Microsoft si trova all'interno del tunnel, aprire Outlook e provare a scaricare la posta elettronica oppure provare a utilizzare Desktop remoto per il server. Se questo non funziona, e si dispone della risoluzione corretta dei nomi, è molto probabile che il problema sia la frammentazione.
2. Da un dispositivo Windows utilizzare quanto segue: C:**> ping -f -l dimensioni_pacchetto_in_byte indirizzo_IP_destinazione**.L'opzione **-f** viene usata per specificare che il pacchetto non può essere frammentato. L'opzione **-l** viene usata per specificare la lunghezza del pacchetto. Provare anzitutto con un pacchetto di dimensioni 1.500. Ad esempio, ping **-f -l 1500 192.168.100**. Se è richiesta la frammentazione ma non è possibile eseguirla, viene visualizzato un messaggio come questo: *È necessario frammentare i pacchetti, ma DF è impostato*.
3. Sui router Cisco, eseguire il comando **debug ip icmp** e usare il comando **ping esteso**. Se si vede *ICMP:dst (x.x.x.x) frammentazione richiesta e DF impostato, irraggiungibile inviato a y.y.y*, dove x.x.x.x è un dispositivo di destinazione e y.y.y è il router, un dispositivo intermedio indica che è necessaria la frammentazione, ma poiché il bit DF è stato impostato nella richiesta echo, un dispositivo intermedio non può frammentarlo per inoltrarlo all'hop successivo. In questo caso, diminuire gradualmente le dimensioni MTU dei ping finché non ne trovi una che funzioni.
4. Sulle appliance di sicurezza Cisco, utilizzare un filtro di acquisizione.cisco(config)#`access-list outside_test allow tcp any host 172.22.1.1 eq 80`**Nota:** se si lascia invariata l'origine, l'amministratore potrà monitorare qualsiasi NAT (Network Address Translation).cisco(config)#`access-list outside_test allow tcp host 172.22.1.1 eq 80 any`**Nota:** quando si inverte le informazioni di origine e destinazione, consente l'acquisizione del traffico

di ritorno.`cisco asa(config)# capture outside_interface access-list outside_test interface outside`L'utente deve avviare una nuova sessione con l'applicazione X. Dopo che l'utente ha avviato una nuova sessione X dell'applicazione, l'amministratore ASA deve usare il comando **show capture outside_interface**.

Soluzioni ai problemi di frammentazione

I problemi di frammentazione possono essere risolti in diversi modi. Tali argomenti sono trattati in questa sezione.

Metodo 1: Impostazione MTU statica

L'impostazione MTU statica può risolvere i problemi di frammentazione.

1. **Modifica MTU sul router:**Notare che se si imposta manualmente l'MTU sul dispositivo, questo indica al dispositivo, che agisce come gateway VPN, di frammentare i pacchetti ricevuti prima di proteggerli e di inviarli attraverso il tunnel. È preferibile che il router protegga il traffico e quindi lo frammenti, ma il dispositivo lo frammenta.**Avviso:** se si modificano le dimensioni dell'MTU su una qualsiasi interfaccia del dispositivo, tutti i tunnel terminati su quell'interfaccia vengono eliminati e ricostruiti.Sui router Cisco, usare il comando **ip** mtu per regolare le dimensioni MTU sull'interfaccia su cui si termina la VPN:
```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip mtu MTU_size_in_bytes
```

2. **Modifica MTU su ASA/PIX:**Sui dispositivi ASA/PIX, usare il comando mtu per regolare le dimensioni dell'MTU nella modalità di configurazione globale. Per impostazione predefinita, l'MTU è impostata su 1500. Ad esempio, se sull'appliance di sicurezza dell'utente è presente un'interfaccia denominata *Outside (dove la VPN è terminata)* e si è stabilito (tramite le misure elencate nella sezione Discover Fragmentation) che si desidera utilizzare 1380 come dimensioni del frammento, utilizzare questo comando:
```
security appliance (config)# mtu Outside 1380
```

Metodo 2: Dimensioni massime segmento TCP

Le dimensioni massime del segmento TCP possono risolvere i problemi di frammentazione.

Nota: questa funzione funziona solo con TCP; gli altri protocolli IP devono utilizzare un'altra soluzione per risolvere i problemi di frammentazione IP. Anche se si imposta l'mtu ip sul router, ciò non influisce su ciò che i due host terminali negoziano nell'handshake a tre vie TCP con il valore TCP MSS.

1. **Modifica MSS sul router:**La frammentazione del traffico TCP avviene perché il traffico TCP viene usato normalmente per trasportare grandi quantità di dati. Il protocollo TCP supporta una funzione denominata TCP maximum segment size (MSS) che consente ai due dispositivi di negoziare una dimensione adatta al traffico TCP. Il valore MSS viene configurato in modo statico su ciascun dispositivo e rappresenta le dimensioni del buffer da utilizzare per un pacchetto previsto. Quando due dispositivi stabiliscono connessioni TCP, confrontano il valore MSS locale con il valore MTU locale nell'handshake a tre vie; il valore più basso viene

inviato al peer remoto. I due peer utilizzano quindi il valore più basso tra i due valori scambiati. Per configurare questa funzionalità, eseguire la procedura seguente:Sui router Cisco, usare il comando **tcp adjust-mss** sull'interfaccia su cui si termina la VPN.

```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip tcp adjust-mss MSS_Size_in_bytes
```

2. **Modifica del valore MSS sull'appliance ASA/PIX:**Per assicurarsi che le dimensioni massime del segmento TCP non superino il valore impostato e che non siano inferiori a una dimensione specificata, usare il comando **syspot connection** in modalità di configurazione globale. Per ripristinare l'impostazione predefinita, utilizzare **la** forma **no** di questo comando. Il valore massimo predefinito è 1380 byte. La funzionalità minima è disabilitata per impostazione predefinita (impostata su 0).Per modificare il limite massimo predefinito di MSS, procedere come segue:

   ```
   security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes
   ```

   Nota: se si imposta una dimensione massima superiore a 1380, i pacchetti possono essere frammentati, a seconda della dimensione MTU (che per impostazione predefinita è 1500). Quando si utilizza la funzione Protezione contro frodi, un numero elevato di frammenti può influire sulle prestazioni dell'appliance di sicurezza. Se si impostano le dimensioni minime, il server TCP non potrà inviare molti pacchetti di dati TCP di piccole dimensioni al client e ciò influirà sulle prestazioni del server e della rete.Per modificare il limite minimo di MSS, procedere come segue:

   ```
   security appliance (config)# sysopt connection tcp-mss minimum MSS_size_in_bytes
   ```

   appliance di sicurezza (config)# `connessione di sistema tcp-mss valore minimo MSS_size_in_bytes`**Nota: per** ulteriori informazioni, fare riferimento alla sezione Configurazione MPF del documento PIX/ASA 7.X in cui si chiede di consentire l'uso di pacchetti che superano il valore MSS: MSS superato - I client HTTP non possono cercare in alcuni siti Web ulteriori informazioni per consentire ai pacchetti MSS superati un altro metodo.

Metodo 3: PMTUD (Path MTU Discovery)

La funzionalità PMTUD può risolvere i problemi di frammentazione.

Il problema principale del parametro TCP MSS è che l'amministratore deve sapere quale valore configurare sul router in modo da evitare la frammentazione. Questo può essere un problema se tra l'utente e la posizione della VPN remota esistono più percorsi oppure, quando si esegue la query iniziale, si rileva che la seconda o la terza MTU più piccola, anziché la più piccola, è basata sulla decisione di routing utilizzata nella query iniziale. La funzionalità PMTUD permette di determinare un valore MTU per i pacchetti IP e di evitare la frammentazione. Se i messaggi ICMP sono bloccati da un router, l'MTU del percorso viene interrotta e i pacchetti con bit DF impostato vengono scartati. Usare il comando **set ip df** per annullare il bit DF e consentire la frammentazione e l'invio del pacchetto. La frammentazione può rallentare la velocità di inoltro dei pacchetti sulla rete, ma gli elenchi degli accessi possono essere utilizzati per limitare il numero di pacchetti su cui il bit DF viene annullato.

1. Il processo PMTUD può non funzionare per tre motivi:Un router intermedio può eliminare il pacchetto e non rispondere con un messaggio ICMP. Questa condizione non è molto comune su Internet, ma può essere comune all'interno di una rete in cui i router sono configurati per non rispondere con messaggi ICMP "destinazione irraggiungibile".Un router intermedio può rispondere con un messaggio ICMP "destinazione irraggiungibile" ma, nel

flusso di ritorno, un firewall blocca questo messaggio. Si tratta di un evento più comune.Il messaggio ICMP "destinazione irraggiungibile" torna all'origine, ma l'origine ignora il messaggio di frammentazione. Questa è la più insolita delle tre questioni.Se si verifica il primo problema, è possibile annullare il bit DF nell'intestazione IP inserita dall'origine oppure regolare manualmente le dimensioni del valore TCP MSS. Per annullare il bit DF, un router intermedio deve modificare il valore da 1 a 0. In genere, questa operazione viene eseguita da un router della rete prima che il pacchetto esca dalla rete. Questa è una semplice configurazione di codice che esegue questa operazione su un router basato su IOS:

```
Router (config) # access-list ACL_# permit tcp any any
Router (config) # route-map route_map_name permit seq#
Router (config-route-map) # match ip address ACL_#
Router (config-route-map) # set ip df 0
Router (config-route-map) # exit
Router (config) # interface type [slot#/]port #
Router (config-if) # ip policy router-map route_map_name
```

2. **Tunnel PMTUD e GRE**per impostazione predefinita, un router non esegue il PMTUD sui pacchetti del tunnel GRE che ha generato lui stesso. Per abilitare il PMTUD sulle interfacce del tunnel GRE e fare in modo che il router partecipi al processo di tuning MTU per i dispositivi di origine/destinazione per il traffico che attraversa il tunnel, utilizzare questa configurazione:Router (config) # `interface tunnel` tunnel_#Router (config-if) # `tunnel path-mtu-discovery`Il comando **tunnel path-mtu-discovery** abilita il PMTUD sull'interfaccia del tunnel GRE di un router. Il parametro opzionale age-timer specifica il numero di minuti dopo il quale l'interfaccia del tunnel reimposta le dimensioni MTU massime rilevate, meno 24 byte per l'intestazione GRE. Se si specifica *infinite* per il timer, il timer non viene utilizzato. Il parametro min-mtu specifica il numero minimo di byte che costituiscono il valore MTU.
3. **PIX/ASA 7.x - Clear Don't Fragment (DF) (Non frammentare)** o gestire pacchetti o file di grandi dimensioni.Non è ancora possibile accedere correttamente a Internet, ai file di grandi dimensioni o alle applicazioni tramite il tunnel perché viene visualizzato questo messaggio di errore MTU delle dimensioni:

   ```
   PMTU-D packet 1440 bytes greater than effective mtu 1434,
    dest_addr=10.70.25.1, src_addr=10.10.97.55, prot=TCP
   ```

   Per risolvere questo problema, assicurarsi di annullare il bit DF dell'interfaccia esterna del dispositivo. Configurare il criterio DF-bit per i pacchetti IPSec con il comando **crypto ipsec df-bit** in modalità di configurazione globale.

   ```
   pix(config)# crypto ipsec df-bit clear-df outside
   ```

   Il bit DF con la funzione dei tunnel IPSec permette di specificare se l'appliance di sicurezza può cancellare, impostare o copiare il bit `DF (Don't Fragment)` dall'intestazione incapsulata. Il bit DF nell'intestazione IP determina se un dispositivo può frammentare un pacchetto.Utilizzare il comando **crypto ipsec df-bit** in modalità di configurazione globale per configurare l'appliance di sicurezza in modo che specifichi il bit DF in un'intestazione incapsulata.quando si incapsula il traffico IPSec in modalità tunnel, usare l'impostazione `clear-df` per il bit DF. Questa impostazione consente al dispositivo di inviare pacchetti più grandi delle dimensioni MTU disponibili. Inoltre, questa impostazione è appropriata se non si conoscono le dimensioni MTU disponibili.

Nota: se si verificano ancora problemi di frammentazione e pacchetti scartati, facoltativamente, è possibile modificare manualmente le dimensioni dell'MTU con il comando **ip mtu tunnel interface**.

In questo caso, il router frammenta il pacchetto prima di proteggerlo. Questo comando può essere usato in combinazione con PMTUD e/o TCP MSS.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Errore crittografia VPN

Si supponga che il tunnel IPSec sia stato stabilito tra il router e il PIX. Se vengono visualizzati messaggi di errore di crittografia che indicano che i pacchetti sono stati scartati, attenersi alla seguente procedura per risolvere il problema:

1. Eseguire una traccia dello sniffer dal client al server per individuare l'MTU migliore da utilizzare.Èpossibile anche utilizzare il test ping:

   ```
   ping  -l   1400  192.168.1.1 -f
   ```

   192.168.1.1 è l'indirizzo IP del computer remoto.
2. Continuare a ridurre il valore di 1400 di 20 fino a quando non viene fornita una risposta.**Nota:** il valore magico, che nella maggior parte dei casi funziona, è 1300.
3. Una volta raggiunta la dimensione massima appropriata del segmento, regolarla in modo appropriato per i dispositivi in uso:Sul firewall PIX:

   ```
   sysopt connection tcpmss 1300
   ```

   Sul router:

   ```
   ip tcp adjust-mss 1300
   ```

Problemi RDP e Citrix

Problema:

È possibile eseguire il ping tra le reti VPN, ma non è possibile stabilire connessioni RDP (Remote Desktop Protocol) e Citrix attraverso il tunnel.

Soluzione:

Il problema può essere dovuto alle dimensioni dell'MTU sul PC dietro l'appliance PIX/ASA. Impostare la MTU su 1300 per il computer client e provare a stabilire la connessione Citrix sul tunnel VPN.

Informazioni correlate

- Risoluzione dei problemi di IP Fragmentation, MTU, MSS e PMTUD con GRE e IPSEC
- PIX/ASA 7.0 Problema: MSS superato - I client HTTP non possono passare ad alcuni siti Web
- Soluzioni per la risoluzione dei problemi più comuni di VPN IPSec di L2L e ad accesso remoto
- Perché non è possibile esplorare Internet quando si utilizza un tunnel GRE
- Documentazione e supporto tecnico – Cisco Systems