L'appliance ASA ha un elevato utilizzo della CPU a causa di un loop del traffico quando i client VPN si disconnettono

Sommario

Introduzione

In questo documento viene descritto un problema comune che si verifica quando i client VPN si disconnettono da un'appliance Cisco Adaptive Security (ASA) che viene eseguita come headend VPN ad accesso remoto. In questo documento viene descritta anche la situazione in cui si verifica un loop di traffico quando gli utenti VPN si disconnettono da un firewall ASA. Questo documento non descrive come configurare o configurare l'accesso remoto alla VPN, ma solo la situazione specifica che deriva da alcune configurazioni di routing comuni.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione della VPN di accesso remoto sull'appliance ASA
- Nozioni base sul routing di layer 3

Componenti usati

Per questo documento, è stato usato uno switch ASA modello 5520 con codice ASA versione 9.1(1).

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.

Prodotti correlati

Questo documento può essere utilizzato con le seguenti versioni hardware e software:

- Qualsiasi modello ASA
- Qualsiasi versione del codice ASA

Premesse

Quando un utente si connette all'ASA come concentratore VPN di accesso remoto, l'ASA installa un percorso basato su host nella tabella di routing ASA che instrada il traffico diretto al client VPN in uscita dall'interfaccia esterna (verso Internet). Quando l'utente si disconnette, il percorso viene rimosso dalla tabella e i pacchetti sulla rete interna (destinati all'utente VPN disconnesso) possono essere scambiati tra l'ASA e un dispositivo di routing interno.

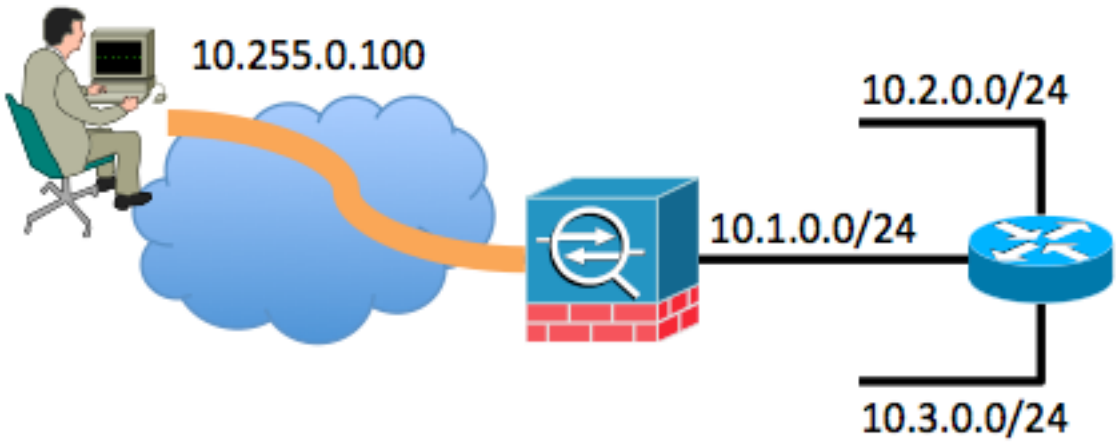
Un altro problema è che i pacchetti broadcast diretti (generati dalla rimozione dei client VPN) potrebbero essere inoltrati dall'ASA come frame unicast verso la rete interna. In questo modo, il pacchetto potrebbe essere inoltrato nuovamente all'ASA, che a sua volta lo rifiuta finché non scade il valore TTL (Time to Live).

In questo documento vengono illustrati questi problemi e vengono illustrate le tecniche di configurazione che possono essere utilizzate per prevenirlo.

Problema: Pacchetti destinati a un loop di client VPN disconnesso all'interno della rete interna

Quando un utente VPN ad accesso remoto si disconnette da un firewall ASA, i pacchetti ancora presenti nella rete interna (destinati agli utenti disconnessi) e l'indirizzo VPN IP assegnato potrebbero diventare loop nella rete interna. Questi loop di pacchetto possono causare un aumento dell'uso della CPU sull'appliance ASA finché il loop non si arresta a causa della riduzione del valore TTL IP nell'intestazione del pacchetto IP a 0, oppure finché l'utente non si riconnette e l'indirizzo IP non viene riassegnato a un client VPN.

Per comprendere meglio questo scenario, considerare la topologia seguente:



Nell'esempio, al client di accesso remoto è stato assegnato l'indirizzo IP 10.255.0.100. L'ASA nell'esempio è collegata allo stesso segmento di rete interno con un router. Al router sono collegati due segmenti di rete aggiuntivi di layer 3. Negli esempi vengono mostrate le configurazioni dell'interfaccia (routing) e della VPN dell'ASA e del router.

Nell'esempio seguente vengono mostrate le evidenziazioni della configurazione dell'ASA:

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0
!
same-security-traffic permit intra-interface
!
ip local pool VPNpool 10.255.0.1-10.255.0.255
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
route inside 10.0.0.0 255.0.0.0 10.1.0.2
```

Nell'esempio seguente vengono mostrati gli elementi di rilievo della configurazione del router:

```
interface FastEthernet0
description connected to the inside interface of the ASA G0/1
ip address 10.1.0.2 255.255.255.0
!
interface FastEthernet1
 description connected to network segment
 ip address 10.2.0.1 255.255.255.0
!
interface FastEthernet2
 description connected to other network segment
 ip address 10.3.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
```

La tabella di routing del router collegato all'interno dell'ASA ha solo un percorso predefinito indirizzato all'interfaccia interna dell'ASA di 10.1.0.1.

Mentre l'utente è connesso all'ASA tramite VPN, la tabella di routing dell'ASA mostra quanto

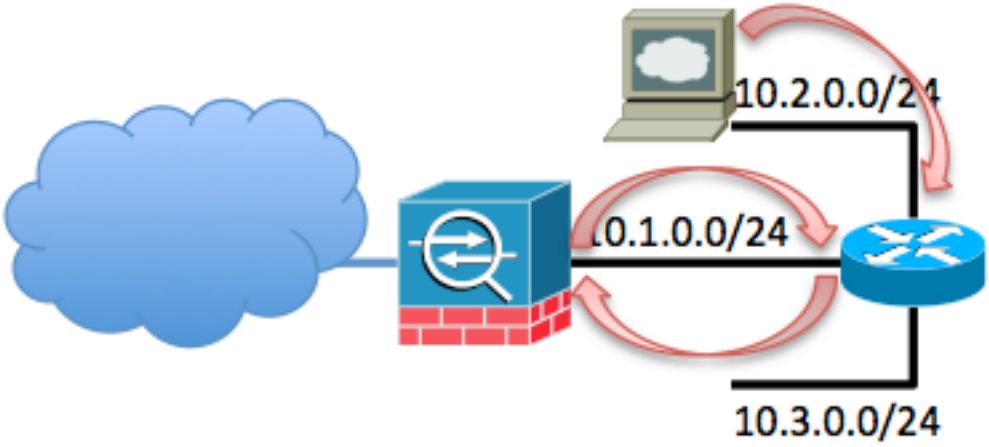
segue:

```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Il problema si verifica quando l'utente VPN di accesso remoto si disconnette dalla VPN. A questo punto, il percorso basato su host viene rimosso dalla tabella di routing dell'ASA. Se un host all'interno della rete tenta di inviare il traffico al client VPN, il traffico viene instradato all'interfaccia interna dell'ASA dal router. Questa serie di fasi si verifica:

1. Il pacchetto destinato a 10.255.0.100 arriva sull'interfaccia interna dell'appliance ASA.
2. Vengono eseguiti controlli ACL standard.
3. La tabella di routing ASA viene controllata per determinare l'interfaccia di uscita per questo traffico.
4. La destinazione del pacchetto corrisponde al percorso 10.0.0.0/8 che punta dall'interfaccia interna verso il router.
5. L'ASA verifica se il traffico è autorizzato - cerca **lo stesso** tipo di **sicurezza per l'interfaccia** e lo trova.
6. Una connessione viene stabilita tra l'interfaccia interna e la connessione stessa e il pacchetto viene inviato al router come hop successivo.
7. Il router riceve un pacchetto destinato alla versione 10.255.0.100 sull'interfaccia verso cui è collegata l'ASA. Il router controlla la tabella di routing per individuare l'hop successivo appropriato. Il router rileva che l'hop successivo è l'interfaccia interna dell'ASA e il pacchetto viene inviato all'ASA.
8. Tornare al passo 1.

Di seguito è riportato un esempio:



Questo ciclo si verifica finché il valore TTL del pacchetto non diminuisce a 0. Si noti che il firewall ASA **non** diminuisce il valore TTL per impostazione predefinita quando elabora un pacchetto. Il router diminuisce il valore TTL mentre instrada il pacchetto. In questo modo si impedisce il verificarsi di questo loop per un periodo di tempo indefinito, ma questo loop aumenta il carico di traffico sull'appliance ASA e provoca un picco nell'utilizzo della CPU.

Problema: I pacchetti broadcast diretti (rete) generati dai client VPN vengono trasmessi su una rete interna

Questo problema è simile al primo. Se un client VPN genera un pacchetto di trasmissione indirizzato alla subnet IP assegnata (10.255.0.255 nell'esempio precedente), il pacchetto potrebbe essere inoltrato come frame unicast dall'ASA al router interno. Il router interno può quindi inoltrarlo all'ASA, causando il loop del pacchetto fino alla scadenza del TTL.

Questa serie di eventi si verifica:

1. Il computer client VPN genera un pacchetto destinato all'indirizzo di broadcast di rete 10.255.0.255 e il pacchetto arriva all'appliance ASA.
2. L'ASA tratta il pacchetto come un frame unicast (causato dalla tabella di routing) e lo inoltra al router interno.

3. Il router interno, che tratta il pacchetto anche come frame unicast, diminuisce il valore TTL del pacchetto e lo inoltra all'appliance ASA.

4. Il processo si ripete finché il valore TTL del pacchetto non viene ridotto a 0.

Soluzioni al problema

Ci sono diverse possibili soluzioni a questo problema. A seconda della topologia di rete e della situazione specifica, una soluzione potrebbe essere più facile da implementare di un'altra.

Soluzione 1 - Percorso statico per interfaccia Null0 (ASA versione 9.2.1 e successive)

Quando si invia il traffico a un'interfaccia **Null0**, i pacchetti destinati alla rete specificata vengono

scartati. Questa funzione è utile quando si configura il protocollo RTBH (Remote Triggered Black Hole) per il protocollo BGP (Border Gateway Protocol). In questa situazione, se si configura una route verso Null0 per la subnet del client di accesso remoto, l'ASA scarta il traffico destinato agli host di tale subnet se non è presente una route più specifica (fornita da Reverse Route Injection).

```
route Null0 10.255.0.0 255.255.255.0
```

Soluzione 2 - Utilizzare un pool IP diverso per i client VPN

Questa soluzione consiste nell'assegnare agli utenti VPN remoti un indirizzo IP che non si sovrapponga ad alcuna subnet della rete interna. In questo modo, l'ASA non potrà inoltrare i pacchetti destinati alla subnet VPN al router interno se l'utente VPN non è connesso.

Soluzione 3 - Rendere la tabella di routing ASA più specifica per i percorsi interni

Questa soluzione è garantire che la tabella di routing dell'ASA non abbia route molto ampie che si sovrappongono al pool IP della VPN. Per questo esempio di rete specifico, rimuovere la route 10.0.0.0/8 dall'appliance ASA e configurare route statiche più specifiche per le subnet che risiedono all'esterno dell'interfaccia interna. A seconda del numero di subnet e della topologia di rete, potrebbe trattarsi di un numero elevato di route statiche e ciò potrebbe non essere possibile.

Soluzione 4 - Aggiungere una route più specifica per la subnet VPN all'esterno dell'interfaccia esterna

Questa soluzione è più complicata delle altre descritte in questo documento. Cisco consiglia di provare a utilizzare le altre soluzioni innanzitutto a causa della situazione descritta nella nota più avanti in questa sezione. Questa soluzione permette di evitare che l'ASA inoltri i pacchetti IP provenienti dalla subnet VPN IP al router interno; a tale scopo, è possibile aggiungere un percorso più specifico per la subnet VPN dall'interfaccia esterna. Poiché questa subnet IP è riservata agli utenti VPN esterni, i pacchetti con un indirizzo IP di origine da questa subnet IP VPN non devono mai arrivare in entrata sull'interfaccia interna dell'ASA. Il modo più semplice per ottenere questo risultato è aggiungere un percorso per il pool IP VPN di accesso remoto dall'interfaccia esterna con un indirizzo IP dell'hop successivo del router ISP upstream.

In questo esempio di topologia di rete la route avrà il seguente aspetto:

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

Oltre a questa route, aggiungere il comando **ip verify reverse-path** all'interno per fare in modo che l'ASA ignori tutti i pacchetti ricevuti sull'interfaccia interna provenienti dalla subnet VPN IP a causa del percorso più preferito esistente sull'interfaccia esterna:

```
ip verify reverse-path inside
```

Dopo aver implementato questi comandi, la tabella di routing ASA ha un aspetto simile al seguente quando l'utente è connesso:

```
ASA# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
S 10.255.0.0 255.255.255.0 [1/0] via 198.51.100.1, outside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Quando il client VPN è connesso, la route basata su host a tale indirizzo IP VPN è presente nella tabella ed è preferibile. Quando il client VPN si disconnette, il traffico proveniente dall'indirizzo IP del client che arriva all'interfaccia interna viene confrontato con la tabella di routing e scartato a causa del comando **ip verify reverse-path inside**.

Se il client VPN genera una trasmissione di rete diretta alla subnet IP della VPN, il pacchetto viene inoltrato al router interno e inoltrato di nuovo dal router all'appliance ASA, dove viene scartato a causa del comando **ip verify reverse-path inside**.

> **Nota:** Dopo l'implementazione della soluzione, se nella configurazione è presente il comando same-security allow intra-interface e i criteri di accesso lo consentono, il traffico proveniente da un utente VPN e destinato a un indirizzo IP nel pool IP della VPN per un utente non connesso potrebbe essere reindirizzato all'esterno dell'interfaccia in formato non crittografato. Si tratta di una situazione rara che può essere risolta utilizzando filtri VPN all'interno dei criteri VPN. Questa situazione si verifica solo se il comando **intra-interfaccia allow con lo stesso livello di sicurezza** è presente nella configurazione dell'ASA.
>
> Analogamente, se gli host interni generano traffico destinato a un indirizzo IP del pool VPN e l'indirizzo IP non è assegnato a un utente VPN remoto, il traffico potrebbe raggiungere l'esterno dell'ASA in formato testo non crittografato.