ASA 8.X: Consenti l'esecuzione dell'applicazione utente con la ridefinizione del tunnel VPN L2L

Sommario

Introduzione

In questo documento viene descritto come usare la funzionalità Flussi tunnel IPSec permanenti e come mantenere il flusso TCP durante l'interruzione di un tunnel VPN.

Prerequisiti

Requisiti

I lettori di questo documento devono avere una conoscenza di base di come funziona la VPN. Per ulteriori informazioni, fare riferimento a questi documenti:

- Esempio di configurazione della VPN L2L
- VPN L2L con ASA

Componenti usati

Per la stesura del documento, è stata usata la versione 8.2 di Cisco Adaptive Security Appliance (ASA) e successive.

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

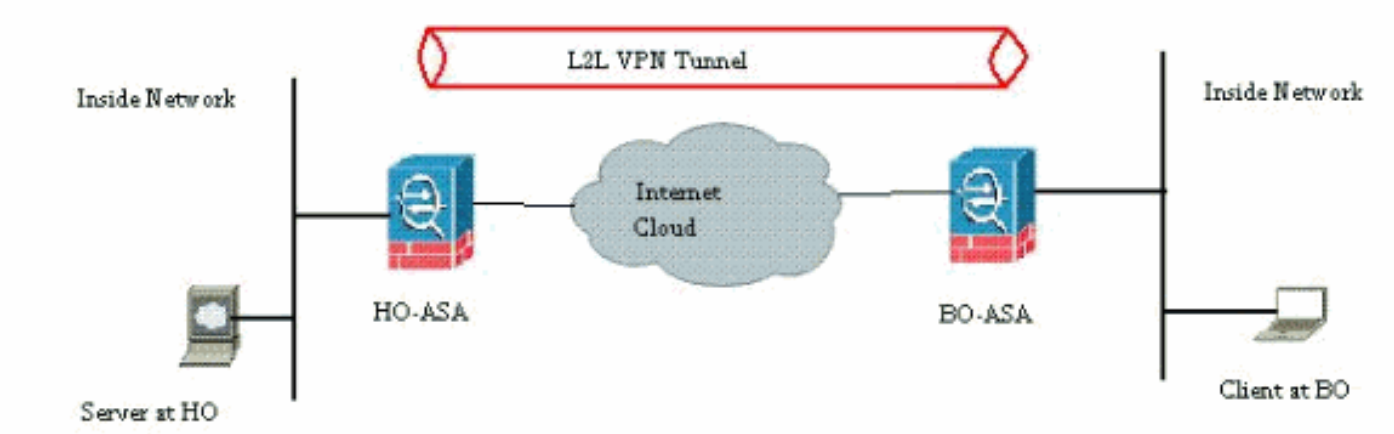
Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

Come mostrato nel diagramma di rete, la succursale (BO) è collegata alla sede centrale (HO) tramite la VPN da sito a sito. Si supponga che un utente della succursale stia tentando di scaricare un file di grandi dimensioni dal server della sede centrale. Il download dura ore. Il trasferimento dei file funziona correttamente finché la VPN non funziona correttamente. Tuttavia, quando la VPN viene interrotta, il trasferimento dei file viene bloccato e l'utente deve riavviare la richiesta di trasferimento dei file dall'inizio dopo aver stabilito il tunnel.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Il problema è causato dalla funzionalità integrata dell'appliance ASA. L'ASA controlla tutte le connessioni che passano attraverso di essa e mantiene una voce nella relativa tabella di stato in base alla funzione di ispezione dell'applicazione. I dettagli del traffico crittografato che passano attraverso la VPN vengono gestiti sotto forma di database delle associazioni di sicurezza (SA). Nello scenario di questo documento, vengono mantenuti due flussi di traffico diversi. Uno è il traffico crittografato tra i gateway VPN e l'altro è il flusso di traffico tra il server alla sede centrale e l'utente finale alla succursale. Quando la VPN viene terminata, i dettagli del flusso per questa particolare associazione di protezione vengono eliminati. Tuttavia, la voce della tabella di stato gestita dall'ASA per questa connessione TCP non è più aggiornata a causa dell'assenza di attività che impedisce il download. Ciò significa che l'ASA manterrà la connessione TCP per quel particolare flusso mentre l'applicazione utente termina. Tuttavia, le connessioni TCP diventeranno isolate e alla fine si verificherà un timeout dopo la scadenza del timer di inattività TCP.

Per risolvere il problema, è stata introdotta una funzionalità denominata Flussi di tunneling IPSec permanenti. Nell'appliance Cisco ASA è stato integrato un nuovo comando per conservare le

informazioni della tabella dello stato durante la rinegoziazione del tunnel VPN. Il comando è mostrato di seguito:

```
sysopt connection preserve-vpn-flows
```

Per impostazione predefinita, questo comando è disattivato. Abilitando questa opzione, Cisco ASA manterrà le informazioni della tabella di stato TCP quando la VPN da L2L si ristabilirà dopo l'interruzione e ristabilirà il tunnel.

Questo comando deve essere abilitato su entrambe le estremità del tunnel. Se il dispositivo non è Cisco all'altra estremità, è sufficiente abilitare questo comando sull'appliance Cisco ASA. Se il comando è abilitato quando i tunnel erano già attivi, è necessario cancellare i tunnel e ristabilirli per rendere effettivo il comando. Per ulteriori informazioni sulla cancellazione e il ripristino dei tunnel, fare riferimento a Cancella le associazioni di sicurezza.

Dettagli sulla compatibilità per questa funzionalità

Questa funzione è stata introdotta nel software Cisco ASA versione 8.0.4 e successive. Questa opzione è supportata solo per questi tipi di VPN:

- Tunnel da LAN a LAN
- Tunnel di accesso remoto in modalità di estensione di rete (NEM)

Questa funzionalità non è supportata per questi tipi di VPN:

- Tunnel di accesso remoto IPSec in modalità client
- Tunnel AnyConnect o SSL VPN

Questa funzionalità non esiste nelle seguenti piattaforme:

- Cisco PIX con software versione 6.0
- Cisco VPN concentrator
- Piattaforme Cisco IOS®

L'abilitazione di questa funzione non crea alcun sovraccarico aggiuntivo sull'elaborazione interna della CPU dell'appliance ASA perché manterrà le stesse connessioni TCP del dispositivo quando il tunnel è attivo.

Nota: questo comando è applicabile solo alle connessioni TCP. Non ha alcun effetto sul traffico UDP. Le connessioni UDP scadranno in base al periodo di timeout configurato.

Configurazioni

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nel documento viene usata questa configurazione:

- Cisco ASA

Di seguito viene riportato un esempio di output della configurazione del firewall Cisco ASA su un'estremità del tunnel VPN:

Cisco ASA

```
ASA Version 8.2(1)
!
hostname CiscoASA
domain-name example.com
enable password <removed>
passwd <removed>
names
!
interface Ethernet0/0
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.248
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.224.9.5 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.224.14.10 255.255.255.0
!
boot system disk0:/asa822-k8.bin
ftp mode passive
 !---Output Suppressed ! access-list test extended
permit ip 10.224.228.0 255.255.255.128 any access-list
test extended permit ip 10.224.52.0 255.255.255.128 any
access-list 100 extended permit ip 10.224.228.0
255.255.255.128 any access-list 100 extended permit ip
10.224.52.0 255.255.255.128 any access-list
inside_access_out extended permit ip any 10.224.228.0
255.255.255.1 ! !---Output Suppressed global (outside) 1
interface nat (inside) 0 access-list test nat (inside) 1
10.224.10.0 255.255.255.0 ! !---Output Suppressed route
inside 10.0.0.0 255.0.0.0 10.224.9.1 1 route outside
0.0.0.0 255.255.255.255 209.165.201.1 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout sip-provisional-media 0:02:00
uauth 0:05:00 absolute timeout tcp-proxy-reassembly
0:01:00 dynamic-access-policy-record DfltAccessPolicy !
!---Output Suppressed http server idle-timeout 40 http
10.224.3.0 255.255.255.0 management http 0.0.0.0 0.0.0.0
inside ! snmp-server enable traps snmp authentication
linkup linkdown coldstart ! !--- To preserve and resume
```

```
stateful (TCP) tunneled IPsec LAN-to-LAN traffic within
the timeout period after the tunnel drops and recovers.
sysopt connection preserve-vpn-flows
service resetoutside
!
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256
esp-md5-hmac
crypto ipsec transform-set testSET esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 209.165.200.10
crypto map map1 5 set transform-set testSET
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 5
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
!---Output Suppressed ! telnet timeout 5 ssh timeout 5
console timeout 0 threat-detection basic-threat threat-
detection statistics access-list ! !---Output Suppressed
! tunnel-group 209.165.200.10 type ipsec-l2l tunnel-
group 209.165.200.10 ipsec-attributes pre-shared-key *
!---Output Suppressed class-map inspection_default match
default-inspection-traffic ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp !
service-policy global_policy global prompt hostname
state Cryptochecksum:5c228e7131c169f913ac8198ecf8427e :
end
```

Abilita questa funzionalità

Per impostazione predefinita, questa funzione è disabilitata. È possibile abilitare questa funzione usando questo comando dalla CLI dell'ASA:

```
CiscoASA(config)#sysopt connection preserve-vpn-flows
```

Per visualizzarlo, usare questo comando:

```
CiscoASA(config)#show run all sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
sysopt connection permit-vpn
sysopt connection reclassify-vpn
sysopt connection preserve-vpn-flows
no sysopt nodnsalias inbound
```

```
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
no sysopt noproxyarp outside
```

Quando si utilizza ASDM, è possibile abilitare questa funzione seguendo il percorso:

Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Opzioni di sistema.

Quindi, selezionare l'opzione *Mantieni flussi VPN con stato quando il tunnel viene rimosso per Network Extension Mode (NEM)*.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

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

- **show asp table vpn-context detail**: visualizza il contenuto del contesto VPN del percorso di sicurezza accelerato, che potrebbe facilitare la risoluzione di un problema. Di seguito viene riportato un output di esempio del comando **show asp table vpn-context** quando la funzionalità dei flussi di tunneling IPSec persistenti è abilitata. Si noti che contiene un flag **PRESERVE** specifico.

```
CiscoASA(config)#show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

Risoluzione dei problemi

In questa sezione vengono presentate alcune soluzioni per evitare il flapping dei tunnel. Vengono inoltre illustrati i pro e i contro delle soluzioni alternative.

Imposta il valore durata IKE su zero

Èpossibile mantenere in vita un tunnel VPN per un periodo di tempo infinito, ma non per ripetere la negoziazione, mantenendo il valore di durata IKE su zero. Le informazioni sull'associazione di protezione vengono conservate dai peer VPN fino alla scadenza della durata. Se si assegna un valore pari a zero, la sessione IKE può durare per sempre. In questo modo è possibile evitare i problemi di disconnessione del flusso intermittente durante la rigenerazione delle chiavi del tunnel. A tale scopo, è possibile usare questo comando:

```
CiscoASA(config)#crypto isakmp policy 50 lifetime 0
```

Tuttavia, questo ha uno svantaggio specifico in termini di compromissione del livello di sicurezza del tunnel VPN. La rigenerazione della chiave per la sessione IKE entro intervalli di tempo specificati offre una maggiore sicurezza al tunnel VPN in termini di chiavi di crittografia modificate ogni volta e diventa difficile per qualsiasi intruso decodificare le informazioni.

Nota: la disabilitazione della durata IKE non implica che il tunnel non riesegua affatto la chiave. L'associazione di protezione IPSec verrà tuttavia reimpostata in base all'intervallo di tempo specificato, poiché non può essere impostata su zero. Il valore minimo consentito per la durata di un'associazione di protezione IPSec è 120 secondi, il valore massimo è 214783647 secondi. Per ulteriori informazioni, vedere Durata SA IPSec.

Messaggio di errore quando il tunnel viene interrotto

Quando questa funzionalità non viene utilizzata nella configurazione, Cisco ASA restituisce questo messaggio di registro quando il tunnel VPN viene interrotto:

```
%ASA-6-302014: Disattivare la connessione TCP 57983 per l'esterno:XX.XX.XX.XX/80
all'interno:10.0.0.100/1135 durata 0:00:36 byte 53947 Tunnel disattivato
```

Potete vedere che la ragione è che il **tunnel è stato demolito**.

Nota: per visualizzare questo messaggio, è necessario abilitare la registrazione di livello 6.

Differenze tra questa funzione e l'opzione reclassify-vpn

L'opzione preserve-vpn-flow viene utilizzata quando un tunnel salta. In questo modo, una precedente connessione TCP rimane aperta e, quando il tunnel ritorna, è possibile usare la stessa connessione.

Quando si usa il comando **syspot connection reclassify-vpn**, cancella qualsiasi flusso precedente relativo al traffico tunneled e classifica il flusso in modo che passi attraverso il tunnel. L'opzione reclassify-vpn viene utilizzata in una situazione in cui è già stato creato un flusso TCP non correlato alla VPN. In questo modo, il traffico non attraversa il tunnel dopo aver stabilito la VPN. Per ulteriori informazioni su questo argomento, fare riferimento a sysopt reclassify-vpn.

Informazioni correlate

- VPN da sito a sito (L2L) con ASA
- Pagina documentazione di Cisco ASA
- Documentazione e supporto tecnico – Cisco Systems