ASA 8.x: Lassen Sie die Benutzeranwendung mit der Wiederherstellung des L2L-VPN-Tunnels laufen

Inhalt

Einführung

Dieses Dokument enthält Informationen zur Funktion "Persistent IPSec Tunneled Flows" und zur Beibehaltung des TCP-Flusses bei Unterbrechung eines VPN-Tunnels.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten sich über die Funktionsweise des VPN im Klaren sein. Weitere Informationen finden Sie in diesen Dokumenten:

- Beispiel für eine L2L-VPN-Konfiguration
- L2L-VPN mit ASA

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Adaptive Security Appliance (ASA) mit Version 8.2 und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

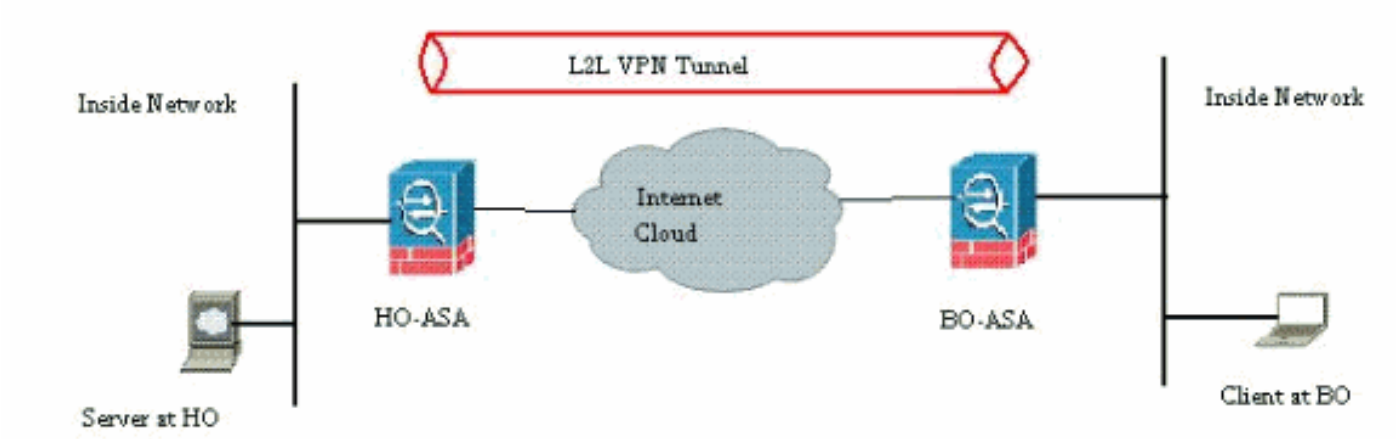
Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

Wie im Netzwerkdiagramm gezeigt, ist die Zweigstelle (BO) über das Site-to-Site-VPN mit der Hauptniederlassung (HO) verbunden. Ein Endbenutzer in der Zweigstelle sollte versuchen, eine große Datei von dem Server in der Hauptniederlassung herunterzuladen. Der Download dauert Stunden. Die Dateiübertragung funktioniert einwandfrei, bis das VPN funktioniert. Wenn das VPN jedoch unterbrochen wird, wird die Dateiübertragung gestoppt, und der Benutzer muss die Dateiübertragungsanforderung von Anfang an nach der Tunneleinrichtung erneut initiieren.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Dieses Problem ergibt sich aus der integrierten Funktionalität der ASA. Die ASA überwacht alle Verbindungen, die sie durchlaufen, und behält entsprechend der Anwendungsinspektionsfunktion einen Eintrag in ihrer Statustabelle bei. Die verschlüsselten Datenverkehrsdetails, die das VPN durchlaufen, werden in Form einer Security Association (SA)-Datenbank verwaltet. Im Szenario dieses Dokuments werden zwei verschiedene Datenverkehrsflüsse verwaltet. Der eine ist der verschlüsselte Datenverkehr zwischen den VPN-Gateways, der andere der Datenverkehrsfluss zwischen dem Server in der Hauptniederlassung und dem Endbenutzer in der Außenstelle. Wenn das VPN beendet wird, werden die Datenflussdetails für diese spezielle SA gelöscht. Der von der ASA für diese TCP-Verbindung gepflegte Eintrag in der Statustabelle ist jedoch veraltet, da keine Aktivität vorliegt, die den Download behindert. Das bedeutet, dass die ASA die TCP-Verbindung für diesen bestimmten Datenfluss beibehalten wird, während die Benutzeranwendung beendet wird. Die TCP-Verbindungen werden jedoch verstreut und nach Ablauf des TCP-Inaktivitäts-

Timers werden sie schließlich deaktiviert.

Dieses Problem wurde durch die Einführung einer Funktion namens Persistent IPSec Tunneled Flows behoben. Ein neuer Befehl wurde in die Cisco ASA integriert, um die Informationen der Statustabelle bei der Neuverhandlung des VPN-Tunnels beizubehalten. Der Befehl wird hier angezeigt:

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

Dieser Befehl ist standardmäßig deaktiviert. Wenn diese Funktion aktiviert ist, erhält die Cisco ASA die TCP-Statustabelle, wenn das L2L VPN nach der Unterbrechung wiederhergestellt wird und den Tunnel wiederhergestellt wird.

In diesem Szenario muss dieser Befehl an beiden Tunnelenden aktiviert werden. Wenn es sich am anderen Ende um ein Gerät handelt, das nicht von Cisco ist, sollte die Aktivierung dieses Befehls auf der Cisco ASA ausreichen. Wenn der Befehl aktiviert ist, während die Tunnel bereits aktiv waren, müssen die Tunnel gelöscht und neu eingerichtet werden, damit dieser Befehl wirksam wird. Weitere Informationen zum Löschen und Wiederherstellen der Tunnel finden Sie unter Löschen der Sicherheitszuordnungen.

Kompatibilitätsdetails für diese Funktion

Diese Funktion wurde in der Cisco ASA-Softwareversion 8.0.4 und höher eingeführt. Dies wird nur für die folgenden VPN-Typen unterstützt:

- LAN-zu-LAN-Tunnel
- Remote Access Tunnel im Network Extension Mode (NEM)

Diese Funktion wird für diese VPN-Typen nicht unterstützt:

- IPSec Remote Access Tunnel im Client-Modus
- AnyConnect oder SSL VPN Tunnel

Diese Funktion ist auf diesen Plattformen nicht verfügbar:

- Cisco PIX mit Softwareversion 6.0
- Cisco VPN Concentrator
- Cisco IOS®-Plattformen

Die Aktivierung dieser Funktion führt nicht zu einer zusätzlichen Überlastung der internen CPU-Verarbeitung der ASA, da die gleichen TCP-Verbindungen wie das Gerät bei Tunnel beibehalten werden.

Hinweis: Dieser Befehl gilt nur für TCP-Verbindungen. Sie hat keine Auswirkungen auf den UDP-Datenverkehr. Die UDP-Verbindungen werden gemäß der konfigurierten Zeitüberschreitungsfrist deaktiviert.

Konfigurationen

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

In diesem Dokument wird diese Konfiguration verwendet:

- CiscoASA

Dies ist ein Beispiel für die Ausführung der Konfigurationsausgabe der Cisco ASA-Firewall an einem Ende des VPN-Tunnels:

CiscoASA

```
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
```

Diese Funktion aktivieren

Diese Funktion ist standardmäßig deaktiviert. Dies kann mithilfe dieses Befehls in der CLI der ASA aktiviert werden:

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

Dies kann mithilfe des folgenden Befehls angezeigt werden:

```
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
```

Bei Verwendung des ASDM kann diese Funktion über folgenden Pfad aktiviert werden:

Konfiguration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options.

Aktivieren Sie anschließend die Option *Beibehalten von zustandsbehafteten VPN-Datenflüssen, wenn der Tunnel für den NEM (Network Extension Mode) verworfen wird*.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show asp table vpn-context detail** - Zeigt die VPN-Kontext-Inhalte des beschleunigten Sicherheitspfads an, was Ihnen bei der Problembehebung helfen kann. Im Folgenden sehen Sie eine Beispielausgabe des Befehls **show asp table vpn-context**, wenn die Funktion für persistente IPSec-getunnelte Datenflüsse aktiviert ist. Beachten Sie, dass es ein bestimmtes **PRESERVE-**Flag enthält.

```
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
```

Fehlerbehebung

In diesem Abschnitt werden einige Problemumgehungen vorgestellt, um das Flapping von Tunneln zu vermeiden. Die Vor- und Nachteile der Workarounds sind ebenfalls detailliert beschrieben.

Legen Sie den IKE-Lebenszeitwert auf Null fest.

Sie können einen VPN-Tunnel für unbegrenzte Zeit ohne Neuaushandlung am Leben erhalten, indem Sie den IKE-Lebenszeitwert auf Null belassen. Die Informationen über die SA werden von den VPN-Peers bis zum Ablauf der Lebensdauer gespeichert. Wenn Sie einen Wert als Null zuweisen, können Sie diese IKE-Sitzung für immer fortsetzen. Auf diese Weise können Sie die zeitweiligen Probleme beim Trennen des Datenflusses während der Neueingabe des Tunnels vermeiden. Dieser Befehl kann verwendet werden:

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

Dies hat jedoch einen besonderen Nachteil hinsichtlich der Beeinträchtigung der Sicherheitsstufe des VPN-Tunnels. Die erneute Keying der IKE-Sitzung innerhalb bestimmter Zeitintervalle erhöht die Sicherheit des VPN-Tunnels in Form von geänderten Verschlüsselungsschlüsseln jedes Mal, und es wird für Eindringlinge schwierig, die Informationen zu dekodieren.

Hinweis: Das Deaktivieren der IKE-Lebensdauer bedeutet nicht, dass der Tunnel überhaupt nicht neu Schlüssel aktiviert. Dennoch wird die IPSec SA im angegebenen Zeitintervall erneut aktiviert, da diese nicht auf Null gesetzt werden kann. Der zulässige Mindestlebensdauerwert für eine IPSec SA beträgt 120 Sekunden, der Höchstwert 214783647 Sekunden. Weitere Informationen hierzu finden Sie unter IPSec SA-Lebensdauer.

Fehlermeldung beim Herunterfahren des Tunnels

Wenn diese Funktion nicht in der Konfiguration verwendet wird, gibt die Cisco ASA diese Protokollmeldung zurück, wenn der VPN-Tunnel unterbrochen wird:

```
%ASA-6-302014: Die TCP-Verbindung 57983 für die Außenstelle:XX.XX.XX.XX/80 nach
innen:10.0.0.100/1135 Dauer 0:00:36 Byte 53947 Tunnel wurde abgebrochen
```

Sie sehen, dass der Grund dafür ist, dass der **Tunnel abgebaut wurde**.

Hinweis: Die Protokollierung auf Stufe 6 muss aktiviert sein, damit diese Meldung angezeigt wird.

Unterschiede zwischen dieser Funktion und der reklassify-vpn-Option

Die Option "bewahrter VPN-Flow" wird verwendet, wenn ein Tunnel abprallt. Dadurch kann ein früherer TCP-Fluss geöffnet bleiben, sodass bei der Wiederherstellung des Tunnels derselbe Fluss verwendet werden kann.

Wenn der Befehl **sysopt connection reklassify-vpn** verwendet wird, löscht er alle vorherigen Datenströme, die sich auf den getunnelten Datenverkehr beziehen, und klassifiziert den Datenfluss für den Tunnelverkehr. Die Option reklassify-vpn wird in einer Situation verwendet, in der bereits ein TCP-Fluss erstellt wurde, der nicht VPN-bezogen ist. Dies führt zu einer Situation, in der der Datenverkehr nach der Einrichtung des VPN nicht über den Tunnel fließt. Weitere Informationen hierzu finden Sie unter sysopt reklassify-vpn.

Zugehörige Informationen

- Site-to-Site-VPN (L2L) mit ASA
- Cisco ASA-Dokumentationsseite
- Technischer Support und Dokumentation - Cisco Systems