ASA 8.X: Allow the User Application to Run with the Re-establishment of the L2L VPN Tunnel

Contents

Introduction

This document provides information about the Persistent IPSec Tunneled Flows feature and how to retain the TCP flow over the disruption of a VPN tunnel.

Prerequisites

Requirements

Readers of this document should have basic understanding on how the VPN works. Refer to these documents for more information:

- Sample L2L VPN Configuration
- L2L VPN with ASA

Components Used

The information in this document is based on the Cisco Adaptive Security Appliance (ASA) with version 8.2 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

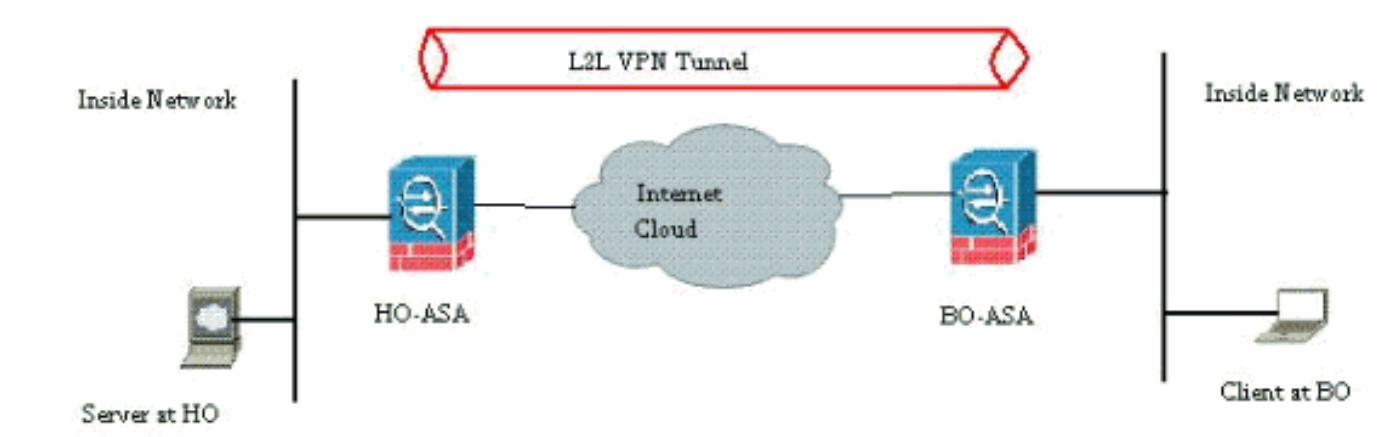
Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

As shown in the network diagram, the branch office (BO) is connected to the head office (HO) through the site-to-site VPN. Consider an end user at the branch office attempting to download a big file from the server situated in the head office. The download lasts hours. The file transfer works fine until the VPN works fine. However, when the VPN is disrupted, the file transfer is hung and the user has to re-initiate the file transfer request again from the beginning after the tunnel is established.

Network Diagram

This document uses this network setup:



This problem arises because of the built-in functionality on how the ASA works. The ASA monitors every connection that passes through it and maintains an entry in its state table according to the application inspection feature. The encrypted traffic details that pass through the VPN are maintained in the form of a security association (SA) database. For this document's scenario, it maintains two different traffic flows. One is the encrypted traffic between the VPN gateways and the other is the traffic flow between the Server at the head office and the end-user at the branch office. When the VPN is terminated, the flow details for this particular SA are deleted. However, the state table entry maintained by the ASA for this TCP connection becomes stale because of no activity, which hampers the download. This means the ASA will still retain the TCP connection for that particular flow while the user application terminates. However, the TCP connections will become stray and eventually timeout after the TCP idle-timer expires.

This problem has been resolved by introducing a feature called Persistent IPSec Tunneled Flows. A new command has been integrated into the Cisco ASA to retain the state table information at

the re-negotiation of the VPN tunnel. The command is shown here:

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

By default, this command is disabled. By enabling this, the Cisco ASA will maintain the TCP state table information when the L2L VPN recovers from the disruption and re-establish the tunnel.

In this scenario, this command has to be enabled on both ends of the tunnel. If it is a non-Cisco device at the other end, enabling this command on the Cisco ASA should suffice. If the command is enabled when the tunnels were already active, the tunnels must be cleared and re-established for this command to take effect. For more details on clearing and re-establishing the tunnels, refer to Clear the Security Associations.

Compatibility Details for this Feature

This feature has been introduced in Cisco ASA software version 8.0.4 and later. This is supported only for these types of VPN:

- LAN to LAN Tunnels
- Remote Access Tunnels in Network Extension Mode (NEM)

This feature is not supported for these types of VPN:

- IPSec Remote Access Tunnels in Client Mode
- AnyConnect or SSL VPN Tunnels

This feature does not exist on these platforms:

- Cisco PIX with software version 6.0
- Cisco VPN Concentrators
- Cisco IOS® platforms

Enabling this feature does not create any additional overload on the internal CPU processing of the ASA because it is going to keep the same TCP connections that the device has when the tunnel is up.

Note: This command is applicable for TCP connections only. It does not have any effect on the UDP traffic. The UDP connections will timeout as per the configured timeout period.

Configurations

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

In this section, you are presented with the information to configure the features described in this document.

This document uses this configuration:

- CiscoASA

This is a sample running configuration output of the Cisco ASA firewall at one end of the VPN tunnel:

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
```

Enable this Feature

By default, this feature is disabled. This can be enabled by using this command at the CLI of the ASA:

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

This can be viewed by using this command:

```
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
```

When using the ASDM, this feature can be enabled by following this path:

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

Then, check the *Preserve stateful VPN flows when the tunnel drops for Network Extension Mode (NEM)* option.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show asp table vpn-context detail**—Shows the VPN context contents of the accelerated

security path, which might help you troubleshoot a problem. The following is a sample output from the **show asp table vpn-context** command when the persistent IPSec tunneled flows feature is enabled. Note that it contains a specific **PRESERVE** flag.`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`

Troubleshoot

In this section, certain workarounds are presented to avoid the flapping of tunnels. The pros and cons of the workarounds are also detailed.

Set the IKE Lifetime Value to Zero

You can make a VPN tunnel stay alive for an infinite time, but not to re-negotiate, by keeping the IKE lifetime value as zero. The information about the SA is retained by the VPN peers until the lifetime expires. By assigning a value as zero, you can make this IKE session last forever. Through this, you can avoid the intermittent flow disconnection issues during the re-keying of the tunnel. This can be done with this command:

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

However, this has a specific disadvantage in terms of compromising the security level of the VPN tunnel. Re-keying the IKE session within specified time intervals provides more security to the VPN tunnel in terms of modified encryption keys each time and it becomes difficult for any intruder to decode the information.

Note: Disabling the IKE lifetime does not mean that the tunnel does not re-key at all. Still, the IPSec SA will re-key at the specified time-interval because that cannot be set to zero. The minimum lifetime value allowed for an IPSec SA is 120 seconds and the maximum is 214783647 seconds. For more information about this, refer to IPSec SA lifetime.

Error Message when Tunnel Drops

When this feature is not used in the configuration, the Cisco ASA returns this log message when the VPN tunnel is disrupted:

```
%ASA-6-302014: Teardown TCP connection 57983 for outside:XX.XX.XX.XX/80 to
inside:10.0.0.100/1135 duration 0:00:36 bytes 53947 Tunnel has been torn down
```

You can see that the reason is that the **Tunnel has been torn down**.

Note: Level 6 logging must be enabled to see this message.

How this Feature Differs with the reclassify-vpn Option

The preserve-vpn-flow option is used when a tunnel bounces. This allows a previous TCP flow to stay open so when the tunnel comes back up, the same flow can be used.

When the **sysopt connection reclassify-vpn** command is used, it clears any previous flow that pertains to the tunneled traffic and classifies the flow to go through the tunnel. The reclassify-vpn

option is used in a situation when a TCP flow was already created that is not VPN related. This creates a situation where traffic does not flow across the tunnel after the VPN is established. For more information about this, refer to sysopt reclassify-vpn.

Related Information

- **Site to Site VPN (L2L) with ASA**
- **Cisco ASA Documentation Page**
- **Technical Support & Documentation - Cisco Systems**