ASA Clientless SSL VPN traffic over IPsec LAN−to−LAN Tunnel Configuration Example

Document ID: 117739

Contributed by Cisco Engineers.
Jul 03, 2014

Contents

Introduction

This document describes how to connect to a Cisco Adaptive Security Appliance (ASA) Clientless SSLVPN Portal and access a server that is located in a remote location connected over an IPsec LAN−to−LAN tunnel.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Clientless SSL VPN Configuration.
- LAN−to−LAN VPN Configuration

Components Used

The information in this document is based on the ASA 5500−X Series that runs Version 9.2(1), but it applies to all ASA versions.

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. Ensure that you understand the potential impact of any command before you make changes on a live network.

Background Information

When traffic from a Clientless SSLVPN session traverses a LAN−to−LAN tunnel, note that there are two connections:

- From the Client to the ASA
- From the ASA to the destination host.

For the ASA−to−destination host connection, the IP address of ASA interface "closest" to the destination host is used. Therefore, the LAN−to−LAN interesting traffic must include a proxy−identity from that interface address to the remote network.

Note: If Smart−Tunnel is used for a bookmark, the IP address of the ASA interface closest to the destination is still used.

Configure

In this diagram, there is a LAN−to−LAN tunnel between two ASAs that allows traffic to pass from 192.168.10.x to 192.168.20.x.

The access−list that determines interesting traffic for that tunnel:

ASA1

```
access−list l2l−list extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0
```

ASA2

```
access−list l2l−list extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
```

If the clientless SSLVPN user tries to communicate with a host on the 192.168.20.x network, ASA1 uses the 209.165.200.225 address as the source for that traffic. Because the LAN−to−LAN Access Control List (ACL) does not contain 209.168.200.225 as a proxy−identity, the traffic is not sent over the LAN−to−LAN tunnel.

In order to send traffic over the LAN−to−LAN tunnel, a new Access Control Entry (ACE) must be added to the interesting traffic ACL.

ASA1

```
access−list l2l−list extended permit ip host 209.165.200.225 192.168.20.0
255.255.255.0
```

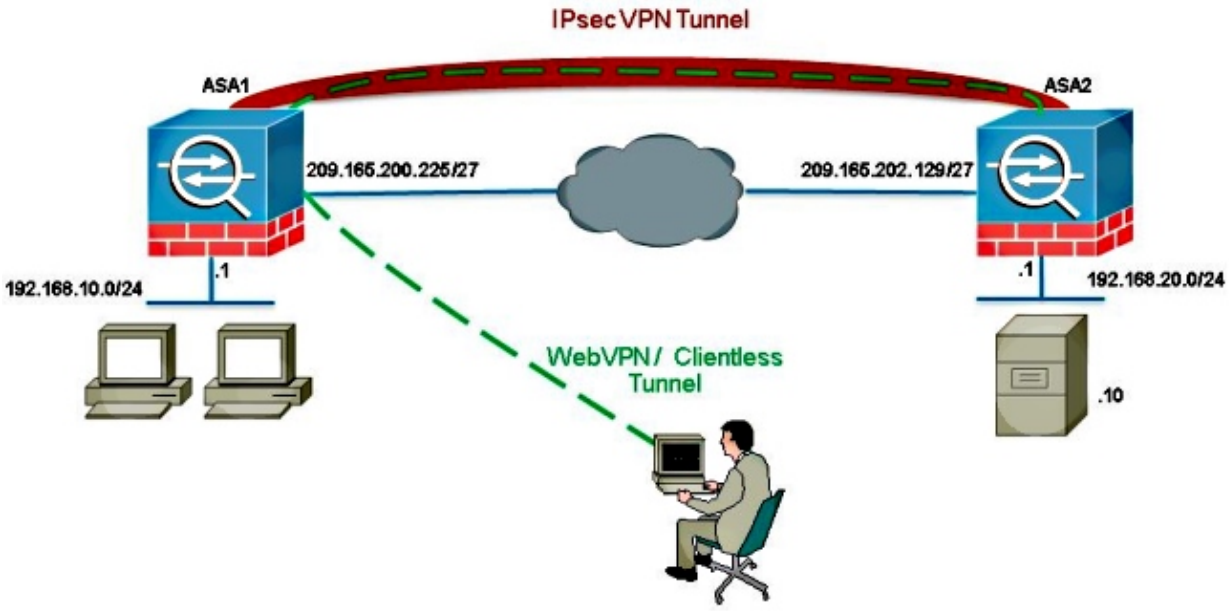
ASA2

```
access−list l2l−list extended permit ip 192.168.20.0 255.255.255.0 host
209.165.200.225
```

This same principle applies to configurations where the Clientless SSLVPN traffic needs to ***u−turn*** out the same interface it came in on, even if it is not supposed to go through a LAN−to−LAN tunnel.

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

Network Diagram



Typically, ASA2 conducts Port Address Translation (PAT) for the 192.168.20.0/24 in order to provide Internet access. In that case, then traffic from 192.168.20.0/24 on ASA 2 should be excluded from the PAT process when it goes to 209.165.200.225. Otherwise, the response would not go through the LAN−to−LAN tunnel. For example:

ASA2

```
nat (inside,outside) source static obj−192.168.20.0 obj−
192.168.20.0 destination
static obj−209.165.200.225 obj−209.165.200.225
!
object network obj−192.168.20.0
nat (inside,outside) dynamic interface
```

Verify

Use this section in order to confirm that your configuration works properly.

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

- ***show crypto ipsec sa***−Verify with this command that a Security Association (SA) between the ASA1 Proxy IP address and the remote network has been created. Check if the encrypted and decrypted counters increase when the Clientless SSLVPN user accesses that server.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

If the Security Association is not built, you can use IPsec debugging to the cause of failure:

- ***debug crypto ipsec <level>***

Note: Refer to Important Information on Debug Commands before you use ***debug*** commands.