Cisco ASA VPN Hairpinning

EDIT:

My Book “Cisco ASA Firewall Fundamentals-3rd Edition” is now available on Amazon as Paperback physical book. MORE INFORMATION HERE

Some time ago a visitor of my website asked me to help him on a special Cisco ASA VPN configuration and thought about sharing it here to help other people as well.

The specific network scenario was the following:

The requirements of the network setup are:

- Two sites connected with IPSEC Site-to-Site VPN over the Internet. Both sites using Cisco ASA firewalls (version 9.x or 8.4).
- **Site1** is the main headquarters site and **Site2** is a remote branch site.
- The LAN networks on each site communicate between them over the IPSEC VPN tunnel.
- Hosts in Site1 (network 192.168.1.0/24) can access the Internet via the local Internet connection through ASA1.
- Hosts in Site2 (network 192.168.2.0/24) can access the Internet ONLY through Site1 via the VPN tunnel. Although there is a local Internet connection on Site2, hosts are not allowed to access the Internet directly. They must come to Site1 (ASA1) over the VPN tunnel and then exit the same ASA1 firewall for accessing the Internet.
- The situation of having VPN traffic entering and exiting the same ASA interface is called **VPN Hairpinning** (or “**VPN on a stick**”).

Scenarios like the above are useful in situations where you want to have centralized control of all Internet access (for hosts in the main site and for hosts in remote branch sites as well). You can implement content filtering, caching, virus protection etc on the central main site and have all the other sites use these centralized resources.

Some key points to have in mind in order to implement the scenario above are the following:

- Since Site2 hosts (private IP addresses) are not allowed to access the Internet locally, you must not configure NAT on ASA2 for translating the private addresses to public. This will prevent them from accessing the Internet.
- On ASA1, you will have traffic from Site2 entering and exiting the same interface (outside interface of firewall). To implement this you must enable “intra-interface” traffic on ASA1, so that traffic can enter and exit the same interface simultaneously. You can do this using the command **“same-security-traffic permit intra-interface”**.
• On ASA1 you must perform PAT on traffic coming from Site2 so that it can access the internet via its outside interface.

• The ACL used for VPN Interesting Traffic on ASA2 must allow 192.168.2.0 towards “any IP”. This is required so that Site2 can access Internet hosts through the VPN tunnel.

• The ACL used for VPN Interesting Traffic on ASA1 must allow “any IP” towards 192.168.2.0. This is required so that returning traffic from Internet hosts can flow through the VPN tunnel towards Site2.

Let’s now see the configuration on both ASA1 and ASA2.

Note: Only relevant configuration is shown.

**ASA1**

```
interface GigabitEthernet0
nameif outside
security-level 0
ip address 20.20.20.1 255.255.255.0
!
interface GigabitEthernet1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0

!Allow intra-interface traffic (to enter and exit same interface)

same-security-traffic permit intra-interface
```
!Configure required network objects

object network obj-local
subnet 192.168.1.0 255.255.255.0
object network obj-remote
subnet 192.168.2.0 255.255.255.0
object network internal-lan
subnet 192.168.1.0 255.255.255.0

!ACL for VPN Interesting Traffic. We allow any IP towards Site2

access-list VPN-ACL extended permit ip any 192.168.2.0 255.255.255.0

!NAT Exemption for VPN traffic between Site1 – Site2

nat (inside, outside) source static obj-local obj-local destination static obj-remote obj-remote

!Configure PAT for local LAN to access the Internet using ASA1 outside interface

object network internal-lan
nat (inside, outside) dynamic interface

!Configure PAT for remote Site2 LAN to access the Internet via ASA1 outside interface

object network obj-remote
nat (outside, outside) dynamic interface

!Configure Site-to-Site IPSEC VPN

crypto ipsec ikev1 transform-set TRSET esp-aes esp-md5-hmac
crypto map VPNMAP 10 match address VPN-ACL
crypto map VPNMAP 10 set peer 30.30.30.1
crypto map VPNMAP 10 set ikev1 transform-set TRSET
crypto map VPNMAP interface outside
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
tunnel-group 30.30.30.1 type ipsec-l2l
tunnel-group 30.30.30.1 ipsec-attributes
ikev1 pre-shared-key cisco123

ASA2

interface GigabitEthernet0
nameif outside
security-level 0
ip address 30.30.30.1 255.255.255.0
!
interface GigabitEthernet1
nameif inside
security-level 100
ip address 192.168.2.1 255.255.255.0

!Configure required network objects

object network obj-local
subnet 192.168.2.0 255.255.255.0
object network obj-remote
subnet 192.168.1.0 255.255.255.0

!ACL for VPN Interesting Traffic. We allow Site2 towards any IP.

access-list VPN-ACL extended permit ip 192.168.2.0 255.255.255.0 any

!NAT Exemption for VPN traffic between Site2 – Site1

nat (inside, outside) source static obj-local obj-local destination static obj-
remote obj-remote
!Configure Site-to-Site IPSEC VPN

crypto ipsec ikev1 transform-set TRSET esp-aes esp-md5-hmac
crypto map VPNMAP 10 match address VPN-ACL
crypto map VPNMAP 10 set peer 20.20.20.1
crypto map VPNMAP 10 set ikev1 transform-set TRSET
crypto map VPNMAP interface outside
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
tunnel-group 20.20.20.1 type ipsec-l2l
tunnel-group 20.20.20.1 ipsec-attributes
ikev1 pre-shared-key cisco123

EDIT:

My Book “Cisco ASA Firewall Fundamentals-3rd Edition” is now available on Amazon as Paperback physical book. MORE INFORMATION HERE

About the Author

Harris Andrea is a Cisco Certified Professional with more than 18 years of experience working with Cisco network technologies. He is the author of two Cisco Books (“Cisco ASA Firewall Fundamentals” and “Cisco VPN Configuration Guide”) which have been embraced by thousands of Cisco professionals all over the world. You can find more Cisco configuration guides and tutorials on his blogs below:
http://www.networkstraining.com
http://www.tech21century.com