Configuring Avaya 9611 VPN for IP Office w/ SOPHOS UTM 9.x

Overview

Some Avaya 9600 phones, such as the 9611, have a native IPsec VPN client that can be used to connect remote workers to the corporate phone system when other options just won't cut it. Online documentation is poor and often differs for each firewall vendor. Please note that this configuration is functional, but it may or may not comply with the security requirements of your business. Please discuss them with your security team and try other settings if necessary.

We are testing this option now to hopefully rid our environment of softphones. We're also testing the "Telecommuter Option" of one-X. This allows our remote workers to use their home phones and proxy everything through the IP Office server, but it comes with the cost of chewing up 2 SIP channels for each call.

Don't forget to buy power injectors!

High Level Network Design

Object	Network/Connection Type	Comment
IPO 8.1	DC Voice Network	
9611 Phones	HQ Voice, Sat Voice, *Home Offices	*This doc…
Soft Phones	HQ Data, Sat Data, *Remote Office	A handful of users…
SOPHOS Firewall	DC	Virtual interfaces for DC Voice and DC Data vLANs
Sat Office Connection	StS IPsec VPN	ASA 5510 – SOPHOS UTM 9.x VM
HQ Office Connection	Gig Fiber – MPLS	Direct Connect from HQ to DC
DC Connection	Dual 10G Fiber	IP Transit secured by SOPHOS HA pair
Remote Workers	Several	Personal connections not managed by IT

Known Issue

The "Enable Direct Media Path" extension option must be unchecked for all extensions participating in a call. Some Avaya documentation says to disable this for "VPN to VPN phone calls", but we experienced the problem with ALL phone calls to/from a VPN phone. Disabling the option for the extension associated with just the VPN phone was not enough. Attempts were made to open firewall rules, verify routes, etc, but nothing yielded the desired result. Talk to your phone support team and ask them if it's okay to disable direct media path for anyone and everyone that will send/receive calls with VPN phones.

- 10 digit extension calls do not experience the issue above because they loop through the outside. However, attempting this is not a good workaround and will only confuse users.
- Every firewall/network configuration will differ. You may not experience the issue, but if you do, try the workaround with a handful of users.

Remote SOPHOS IPsec VPN Setup

1. Create a New IPsec Policy

Description	Setting	Note
Name	VPNPHONE	
IKE encryption algorithm	3DES	
IKE authentication algorithm	SHA1	
IKE SA lifetime	7800	
IKE DH group	Group 2: MODP 1024	
IPsec encryption algorithm	3DES	
IPsec authentication algorithm	SHA1	
IPsec SA lifetime	3600	
IPsec PFS group	Group 2: MODP 1024	
Strict Policy	Unchecked	
Compression	Unchecked	

2. Create a New IPsec Remote Access Rule

Description	Setting	Note
Name	VPNPHONE	
Interface	External (WAN)	Depends on config, but will be the most common selection
Local Networks	***	Add all networks – IP Office & each network w/ phones
Virtual IP Pool	VPN Pool (IPsec)	Defaults to 10.242.4.0/24
Policy	VPNPHONE	
Authentication Type	Preshared Key	Document the key. It will be used for the 9611 too.
Enable XAUTH	SELECTED	
Allowed Users	**	Create new Users – ext01, ext02, etc.

3. Configure Required Firewall ACLs
   a. Outside the scope of this document, but make sure your IPsec VPN group can minimally talk to the network where the IPO(s) server is. Depending on your network and firewall configuration, and the requirements of your security department, one or more simple rules from the IPO network to the IPsec VPN group (and back) might be enough. If you can get direct media access to work you may need to supply all networks where phones are located.

4. Configure the 9611 Phone
   a. Enter the OPTIONS tab on boot up. Our code to enter was 27238. This may or may not be different for you.
   b. Go to the VPN setup and supply the following values:

Phone Option	Value
VPN	Enabled
VPN Vendor	OTHER
Gateway Address	The public IP address applied to the interface of the SOPHOS IPsec VPN

Encapsulation	4500-4500
Copy TOS	Yes
External Phone IP Address	** Typically done by your DHCP server
External Router	** Typically done by your DHCP server
External Subnet Mask	** Typically done by your DHCP server
External DNS Server	** Typically done by your DHCP server
Auth Type	PSK with XAUTH
VPN User Type	Any
VPN User	The VPN user(s) account you created above
Password Type	Save in Flash
User Password	The VPN user(s) account password
IKE ID (Group Name)	VPNPHONE
Pre-Shared Key (PSK)	The PSK you entered for the SOPHOS “IPsec Remote Access Rule”
IKE ID Type	USER_FQDN
IKE Xchg Mode	ID Protect
IKE DH Group	2
IKE Encryption Alg.	3DES
IKE Auth. Alg.	SHA1
IKE Config. Mode	Enabled
IKE PFS DH Group	2
IPsec Encryption Alg	3DES
IPsec Auth. Alg.	SHA-1
Protected Network..	** See extended comments below
IKE over TCP	Auto

**** 9611 Protected Network Comments**

- You should supply all networks that were included in the “Local Networks” of the SOPHOS “IPsec Remote Access Rule”. A lot of confusing documentation, partially accurate, is floating around on the Internet. Some of it even says to use the IP Pool network associated with your VPN group. If you don’t have one or more correct networks listed you will fail on “IKE PHASE 2”. We were getting this error message
    - cannot respond to IPsec SA request because no connection is known for 10.x.x.x/24===209.x.x.x:4500[209.x.x.x]...4.x.x.x:4500[VPNPHONE]===192.x.x.x/32
        - ****Actual addresses were removed…*

- If you do not have “Direct Media Path” enabled on your extensions then you really only need to supply the network(s) where the IPO server(s) is located. See the notes on “Direct Media Path” above for more info.

- Some Avaya documentation says to use 0.0.0.0/0, which means any addressable network. This does not work.

- Multiple networks can be defined in the 9611. Simply list each one with commas and do not use spaces.
    - Example: 192.168.10.0/24,172.16.0.0/16,192.168.30.0/24