Part 1 - VPN

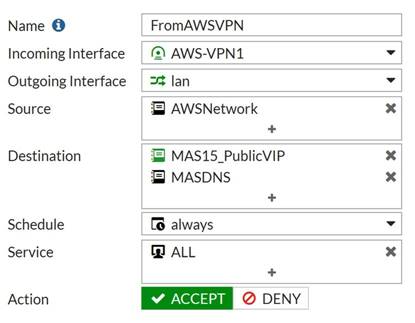
Thursday, February 28, 2019

8:50 AM

Wanted to get some ideas down:

**SSL-VPN Tunnels (site to site)**

From a connectivity perspective, the SSL VPN Tunnels that we have created for, say, Draft Kings, don’t provide DNS resolution on their own. What that means is, as you can see:



Anything coming from AWSNetwork, can reach MAS15PublicVIP and also, now, MASDNS. It also requires them to set the DNS of their machines in AWS to use the MASDNS IP as primary/secondary DNS server, which means that their jumpbox in AWS can reach the MAS 15 portals (thanks to the stub zones set up on MASDNS). Technically, they could also resolve other MAS instances that are held in the stub zones on the MASDNS, but they wouldn’t be able to connect to them, because the firewall policy only allows them access to the MAS15 public VIP space, so we’re fine there I think.

So, the fact that MASDNS has other stub zones to other locations, I don’t see as an issue. I don’t believe it needs a stub/conditional forwarder to the DC01 and DC02 though, that’s unnecessary.

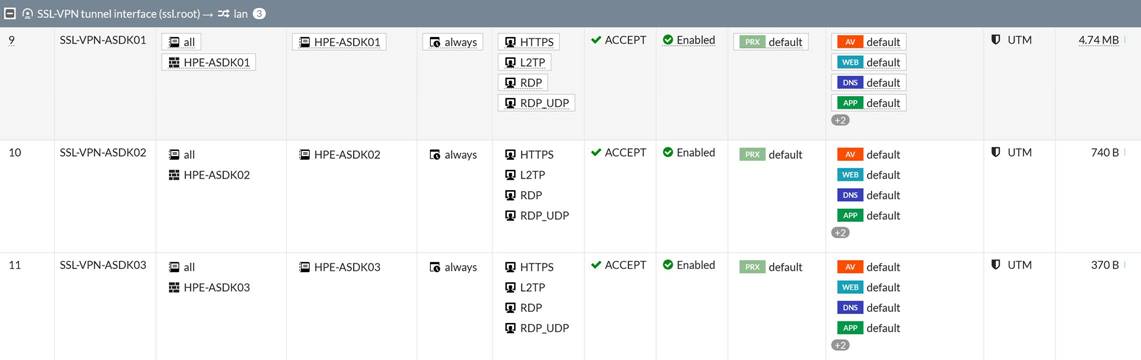
I suspect we will replicate this approach with other customers **who want to connect their site to a particular MAS instance.** If a customer just wants access to a multi-node, but not back to their own site, we’d use the SSL Client connection, below.

**SSL Client Connections**

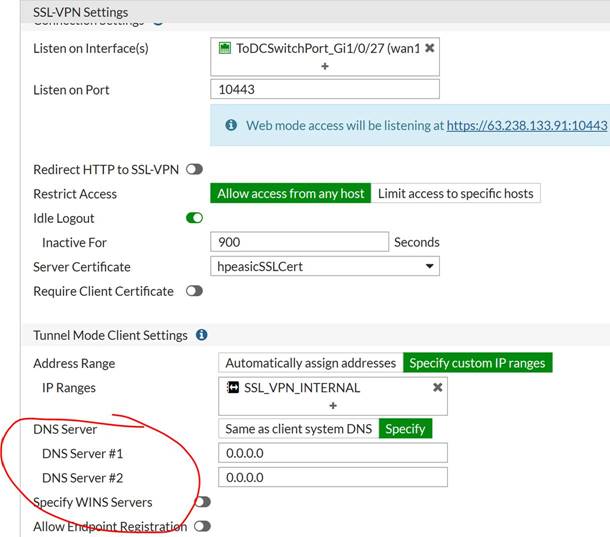
The SSL client connections will be used to connect to the ASDKs, but also when we want to log into the lab in general (we should create a lan-wide policy for us as admins). The SSL client connections will also be used to connect to the Multi-nodes, where a site 2 site connection is not required.

**ASDKs**

In the instance of ASDK access, you’ll create the appropriate IPv4 policies, to correspond to the individual ASDKs. This scopes access appropriately, but also, if I particular user is a member of the AD groups ASDK01, 02, and 03, they’ll be able to access all 3.

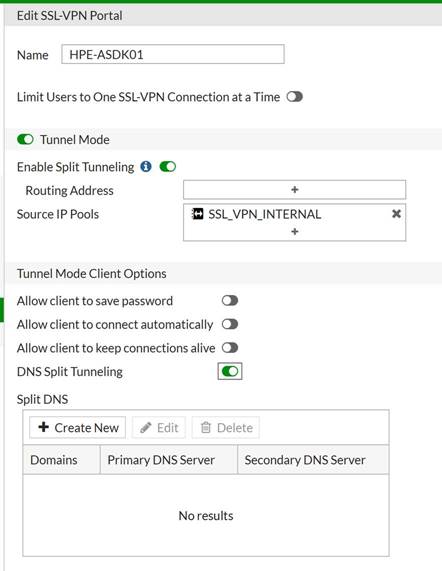


As part of defining these policies, you can, for the **overall SSL settings for the firewall**, set the DNS servers:



This shouldn’t be necessary, seeing as for ASDKs, due to the use of VPN split tunnels, you would use your own native local DNS servers for internet name resolution (set as “Same as client system DNS” above), and once you have connected via VPN, you’ll either RDP to the ASDK host (and thus use it’s local DNS resolution), or you’re connecting the inbox Azure Stack VPN capability, and again, using the inbox DNS from there. Either way, we don’t need to give people who are accessing ASDKs, access to a specific DNS Server. **Note – All ASDKs should be deployed with an external DNS forwarder set during deployment. None of them need to use a 10.1.1.x address for their DNS resolution – best practice will be to set DNS to 1.1.1.1 and 1.0.0.1.**

In addition, if you had a user coming in via VPN, and accessing a multi-node system, to resolve the portal, we’re going to need to give them access to a DNS server to get to the portals. To do this, I *think* we’d need to establish a split DNS tunnel at the VPN Portal level:



We’d have to test this, but I think it would work. So, for instance, if we wanted to give a customer access to MAS15, and they aren’t using a site to site VPN, we’d create the appropriate policy, scoped to the MAS15 public VIP space, and then create a “portal” as shown above, move the DNS Split Tunnel slider, and then add the MASDNS DNS IP to the list. I think. Again, we’d have to test.

VPN Admin Connectivity

Thursday, February 28, 2019

9:23 AM

# Configuration

There is a new local AD security group in the lab, which represents only those accounts that can come through the VPN and have complete LAN access to all ASDKs, MAS systems etc. I wouldn't add GBBs to this one. We should consider scoping the existing Microsoft GBB AD security group to a more specific set of resources, such as the ASDK network, and MAS instances, and not, for instance, the lab servers themselves. Anyway…

Machine generated alternative text:
Lab Admins Properties 
Name 
krenekj 
Matt McSpiltt 
Michael Powers 
Attribute Editor 
Managed By 
Active Directory Domain Services Folder 
hpeasic local/Llseæ 
hpeasic .local/l_lserz 
I-pea sic. local / users 
hpeasic local / users 

This **Lab Admins** group is then attached to a policy in the firewall, through LDAP integration:

Machine generated alternative text:
• • FortiGate IOOE 
Dashboard 
Security Fabric 
FortiView 
+ Network 
System 
Policy & Objects 
a Security Profiles 
VPN 
a User & Device 
User Definition 
User Groups 
Guest Management 
Device Inventory 
HPE-Bellevue-Lab-Firewall 
Edit User Group 
Name 
Type 
Lab Admins 
Firewall 
Members 
Remote Groups 
Edit Delete 
Remote Server 
HPEASIC-DCOI 
HPEASlC-DC02 
Group Name 
CN = Lab Admins,OU -Security Groups, 
CN = Lab Admins,OU -Security Groups, 
Cancel 
Custom Devices & Groups 

And this firewall group is mapped to a policy in the firewall:

Machine generated alternative text:
12 
SSL-VPN tunnel interface (ssl.root) 
SSL-VPN-LabAdmins 
all 
Ian O 
LAB_NETWORK 
always 
DNS 
HTTP 
HTTPS 
L2TP 
ACCEPT 
e Enabled 
default 
default 
default 
default 
O UTM 
* Lab Admins 

This policy essentially allows all members of the Lab Admins AD security group to come through the VPN tunnel, and access the 'Lab Network' which is a 10.0.0.0/8 subnet encompassing the whole LAN essentially. The services that are allowed through this particular tunnel are http/s, L2TP (VPN within the VPN tunnel, for ASDKs), DNS and RDP.

This policy is mapped to a specific VPN 'portal' in the Firewall:

Machine generated alternative text:
• FortiGate IOOE 
Dashboard 
Security Fabric 
FortiView 
+ Network 
System 
Policy & Objects 
a Security Profiles 
VPN 
HPE-Bellevue-Lab-Firewall 
Edit SSL-VPN Portal 
Name 
LABADMINS 
Overlay Controller VPN 
I Psec Tunnels 
I Psec Wizard 
I Psec Tunnel Templates 
SSL-VPN Portals 
SSL-VPN Settings 
a User & Device 
Log & Report 
C Monitor 
Limit Users to One SSL-VPN Connection at a Time 
C) Tunnel Mode 
Enable Split Tunneling O C 
Routing Address 
Source IP Pools 
Tunnel Mode Client Options 
Allow client to save password 
Allow client to connect automatically 
Allow client to keep connections alive C) 
DNS Split Tunneling 
C) Enable Web Mode 
C Enable FortiClient Download 
Download Method 
Customize Download Location C) 
Direct 
SSL-VPN Proxy 

Which has been added to the core SSL VPN Settings (bottom of the screenshot)

Machine generated alternative text:
• • FortiGate IOOE 
Dashboard 
Security Fabric 
FortiView 
+ Network 
System 
Policy & Objects 
a Security Profiles 
VPN 
HPE-Bellevue-Lab-Firewall 
SSL-VPN Settings 
Connection Settings O 
Listen on Interface(s) 
Listen on Port 
Redirect HTTPtoSSL-VPN 
Restrict Access 
Idle Logout 
Inactive For 
Server Certificate 
Require Client Certificate 
Tunnel Mode Client Settings O 
Address Range 
IP Ranges 
DNS Server 
DNS Server #1 
DNS Server 
Specify WI NS Servers 
ToDCSwitchPort_Gi1/O/27 (wanl X 
10443 
O Web mode access will be listeningat https://63.238.133.91:10443 
Overlay Controller VPN 
I Psec Tunnels 
I Psec Wizard 
I Psec Tunnel Templates 
SSL-VPN Portals 
SSL-VPN Settings 
a User & Device 
Log & Report 
C Monitor 
Allow access from any host 
900 
hpeasicSSLCert 
Limit access to specific hosts 
Seconds 
Automatically assign addresses 
Same as client system DNS 
10.1.1.23 
10.1.1.26 
Allow Endpoint Registration 
Authentication/Portal Mapping O 
+ Create New 
Edit Delete 
Users/Groups 
* HPE-ASDK02 
HPE-ASDKOI 
* HPE-ASDK04 
* HPE-ASDK05 
* HPE-ASDK03 
* LabAdmins 
All Other Users/Groups 
Portal 
HPE-ASDK02 
HPE-ASDKOI 
HPE-ASDK04 
HPE-ASDK05 
HPE-ASDK03 
LABADMINS 
web-access 

You'll notice that in the above screenshot, any user coming through the VPN (not just the Lab Admins group) will resolve internal names using 10.1.1.23 and 10.1.1.26. This works fine for resolving hpeasic.local names, and hpeasic.com names, such as the Azure Stack portals etc. Whether or not the users can actually *reach* those locations is ultimately determined by their policy, for instance, members of the HPE-ASDK05 AD group, can resolve hpeasic.local addresses, but they will only ever be able to reach the IP of the ASDK host itself.

* **We should still set up VLANs as an extra layer of isolation.**

# Access via VPN for Lab Admins

* Install FortiGate Client (latest release: <https://www.fortinet.com/support/product-downloads.html>)
* Setup your FortiClient as per below - you can use whatever Connection Name you like.

FortiCIient 
File Help 
mmcspirt 
@ COMPLIANCE & TELEMETRY 
VULNERABILITY SCAN 
REMOTE ACCESS 
O Notifications 
Settings 
O About 
Edit VPN Connection 
VPN 
Connection Narne 
Description 
Rernote Gateway 
Client Certificate 
Authentication 
Username 
VPN 
HPE-ASDKLA3 
https://firewall 
*Add Remote Gateway 
Customize port 10443 
None 
C) Prompt on login Save login 
matt@hpeasiccom 
Do not Warn Invalid Server Certificate 
Cancel 

Login:

FortiCIient 
File Help 
mmcspirt 
@ COMPLIANCE & TELEMETRY 
VULNERABILITY SCAN 
REMOTE ACCESS 
O Notifications 
Settings 
O About 
VPN Narne 
Username 
Password 
HPE-ASDKLAB 
matt@hpeasic.com 

Voila! You should then be connected, and able to RDP directly to resources within the lab, and access the MAS portals of any stamp, assuming you have the root certificate installed on your local machine. No need to go via the jumpbox. In addition, you should be able to reach most resources by name, in case you don't know the IP. You may have to use the full name though, such as hpeasic-dc01.hpeasic.local etc. I don't think just the computername will resolve as the VPN doesn't add a default suffix.

FortiCIient 
File Help 
VPN Connected 
mmcspirt 
@ COMPLIANCE & TELEMETRY 
VULNERABILITY SCAN 
REMOTE ACCESS 
O Notifications 
Settings 
O About 
VPN Name 
IP Address 
Username 
Duration 
Bytes Received 
Bytes Sent 
HPE-ASDKLAB 
192_168.101.1 
matt@hpeasic.com 
0001:28 
14.75 KB 
27.28 KB 
Disconnect 

VPN User Connectivity (Tunnel)

Thursday, February 28, 2019

1:15 PM

# Optimal Connectivity via FortiClient & Azure Stack Native VPN

## Pre-Reqs

* + Ability to install FortiClient VPN software on your workstation/device
  + Ability to install PowerShell 5.1 (on Windows versions older than 10)
  + Ability to import certificates into your workstation trusted root store

For devices that meet the requirements above, the following steps will walk you through how to set up connectivity into the HPE ASIC lab.

## Step 1 - Download FortiClient Software & Configure Lab VPN

* + Visit: <https://www.fortinet.com/support/product-downloads.html> and download the latest version of the FortiClient VPN software for your specific device. Install the software.
  + Once installed, open the FortiClient console, click on **Remote Access**, click on the settings icon, then **Add New Connection.**
  + Complete the details as per the graphic below, adjusting the information to that provided by the instructor:

Machine generated alternative text:
FottiCIient 
File Help 
@ COMPLIANCE & TELEMETRY 
* VULNERABILITY SCAN 
REMOTE ACCESS 
O Notifications 
Settings 
Edit VPN Connection 
HPE-ASDKLA3 
+Add Remote Ga teway 
Customize port 10443 
C) Prompt on login O Save I ogin 
matt@hpeasiccom 
DO not Warn Invalid Server Certificate 

* + Click **Save**, and then back on the **Remote Access** page, ensure that your **VPN Name** is the connection that you just created, enter your **password** provided by the instructor, and click **Connect**.

Machine generated alternative text:
@COMPLIANCE TELEMETRY 
* VULNERABILITY SCAN 
REMOTE ACCESS 
O Notifications 
VPN Nair* 
HPEASDKLAB 
Connect 

* + Once connected, the console may disappear from view. Click the icon in your **System Tray** to bring it to the foreground. Observe the connection details:

Machine generated alternative text:
FortiCIient 
File Help 
VPN Connected 
@ COMPLIANCE & TELEMETRY 
* VULNERABILITY SCAN 
REMOTE ACCESS 
O Notifications 
Settings 
O About 
VPN Name 
IP Address 
Username 
Duration 
Bytes Received 
Bytes Sent 
HPE-ASDKLAB 
192.168.101.1 
matt@hpeasic.com 
7.52 KB 
21.74 KB 
Disconnect 

## Step 2a - Install Azure Stack PowerShell, Tools and Azure Stack VPN (for Windows PCs)

With the VPN established, you will now configure the Azure Stack specific VPN, in order to reach the ASDK host.

### Step 2a.1 - Install the latest Windows PowerShell (for non-Windows 10 PCs)

* + If you are running Windows 10, skip this step.
  + For those PCs on older versions of Windows, you should install version 5.1 of Windows PowerShell from:  
    <http://aka.ms/wmf5download>
  + To install Windows PowerShell 5.1 you may also need to install .NET Framework 4.5 or above. A suitable version is here:  
    <https://go.microsoft.com/fwlink/?LinkId=863262>

### Step 2a.2 - Install the Azure Stack PowerShell Modules, Tools and VPN

* + Note, on machines running **Windows 7**, the script will not work - please speak to your instructor about alternative options.
  + On your system that is now running Windows 8.1 or 10, PowerShell 5.1 and .NET Framework 4.5 or higher, your instructor will provide you with a PowerShell script (AsdkVPN.ps1) to run on your machine. This will install the relevant PowerShell modules (optional), and configure the Azure Stack VPN appropriately based on your user input.
  + To run the script, perform the following:

* + **Open** an **Administrative PowerShell console**
  + Navigate to the location you have stored the AsdkVPN.ps1 script
  + Enter .\AsdkVPN.ps1 and hit enter.
    1. Optional - if you want to install the Azure/Azure Stack PowerShell tools, use -installPowerShell
    2. Optional - if you want to install the GitHub tools, use -installTools
    3. You can use both of those flags at the same time:  
       .\AsdkVPN.ps1 -installPowerShell -installTools

* + Once complete, you should see the VPN connected like so:

OF HPE-ASDK 
Connected 

* + You should now be able to navigate to the portals:
    1. <https://adminportal.local.azurestack.external>
    2. <https://portal.local.azurestack.external>

## Step 2b - Install Azure Stack VPN for Mac

For explaining the connectivity process for a MAC, we’ll be using examples from OS X. The first step, is to install the certificate in your keychain. **Double-click your certificate file provided to you by your instructor**, and in your keychain, you should see a new certificate with a Red X.

Now, because all the services use SSL certificates our MAC OS X need to trust the Azure Stack Certificate Authority. **Click the first option and switch to Always Trust**. And then click the close button (red dot).

To access all the services in the internal Azure Stack you need to add two static routes that will be executed when you connect with the VPN profile.

Create a new script in /etc/ppp/ip-up, for example:

sudo vi /etc/ppp/ip-up

Add the following to the file, and save:

#!/bin/sh

/sbin/route add -net 192.168.102.0/27 -interface $1

/sbin/route add -net 192.168.105.0/27 -interface $1

Now we need to configure our new VPN connection to the Azure Stack Development Kit host - Click your **System Preferences, then Network**:

Machine generated alternative text:



Click the **plus sign (+)** in the lower left corner of the network screen

Machine generated alternative text:



Select **VPN** in the Interface drop down, LT2P over IPSec for **VPN Type** and a name for your VPN connection, for example AzureStackVPN, then click **Create**.

Machine generated alternative text:



On the VPN properties page, leave **Configuration** as Default, type the ASDK Host IP in the **Server Address**, which your instructor will provide you. Your **Account Name** is azurestackadmin (if that fails, use azurestack\azurestackadmin) and click **Authentication Settings**.

Machine generated alternative text:



Then type your password, provided by your instructor, in the **Password** field and **Shared Secret** and click **OK**.

Machine generated alternative text:



Click the **Advanced** button for your VPN connection.

Machine generated alternative text:



Click the **DNS** tab and add **azurestack.local** as a search domain for your VPN connection and click **OK**.

Machine generated alternative text:



Back on the VPN properties page, click **connect**

Machine generated alternative text:



When prompted, type your Azure Stack provided password.

Machine generated alternative text:



Once connected, open your browser and type: <https://adminportal.local.azurestack.external> and login with your supplied @hpeasic.com credentials.

VPN User Connectivity (Web Portal)

Thursday, February 28, 2019

3:14 PM

As an alternative to installing the FortiClient and creating an SSL Tunnel through to the lab environment, an alternative to this approach is to use the firewall web portal.

To access the web portal, visit: <https://firewall.hpeasic.com:10443> and login with your provided credentials:

Please Login 
vpntest@hpeasic.com 
Login 
Y Launch FortiClient 

* Once logged in, click on **Quick Connection** and select **RDP**.
* Complete the details as per below, adjusting for your specific parameters provided by your instructor:

Host 
Port 
Use SSL-VPN Credentials 
Username 
Password 
Keyboard Layout 
Security 
Preconnection I D 
Preconnection Blob 
Load Balancing Information 
10.4.1.21 
3389 
azurestack\azurestackadmin 
English (US). 
TLS encryption. 
2147483648 
Launch 
Cancel 

* Note, it is important to select **TLS encryption** as the chosen encryption.
* You instructor will provide the appropriate IP address, and username/password
* Click **Launch**
* An RDP session should present itself in the browser:

ASDK VPN Portal 
RDP: 104.1.21 
https://firewallhpeasic.com:10443/ssIvpn/remote.html?ld— 
-7a2bb3a5-4516-4c24-ae10-5ed1d2f258f7&theme- 
—blue&lang=en 
Recycle Bin 
a 
Azure Stack 
Admin Portal 
a 
Azure Stack 
user Portal 
Chrome 
Visual Studio 
Code 
WinSCP 
WinDirStat 
Activate Windows 
Go to Settings to activate Windows. 
11:19 PM 
2/28/2019 

* You should be able to navigate to the Admin or User portal using the icons on the desktop.
* **Note - by default, only a single user (azurestack\azurestackadmin) is enabled for RDP access. Use the Active Directory Users and Computers MMC to add other domain users \*\*HOWEVER\*\*, only 2 users can be logged in simultaneously, as this is not an Remote Desktop Services host.**