Barcode / Kiosk Project

Configuring SonicWALL NSA 250M

For

IPsec VPN Tunnel to DET ASA

Includes

Notes on SonicWALL Packet Monitor

&

VBS script for silent CMD ping loop

Prepared By

William Bamber | Metro S/W ETA

Employment & Training Resources

Norwood | Framingham

7/15/2014

Rev B | 8/25/14

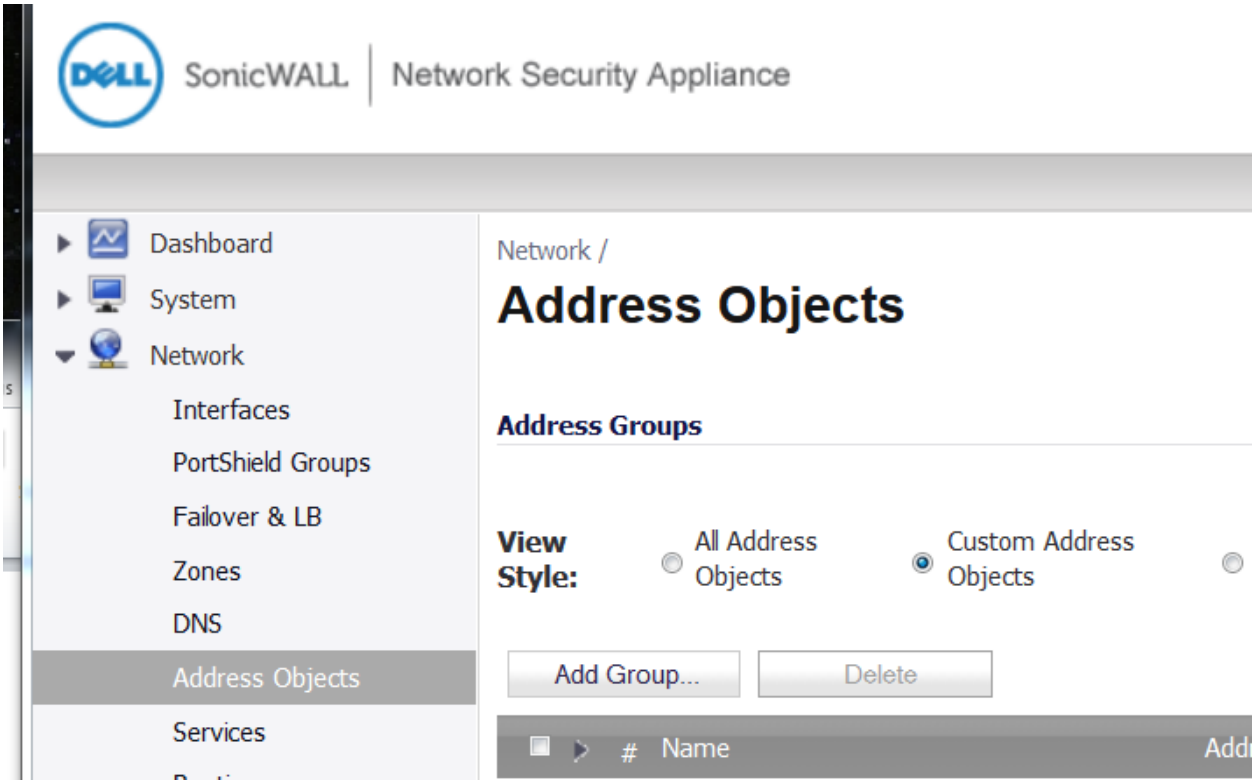
Part 1

Configuring SonicWALL NSA 250M for IPsec VPN Tunnel to DET ASA

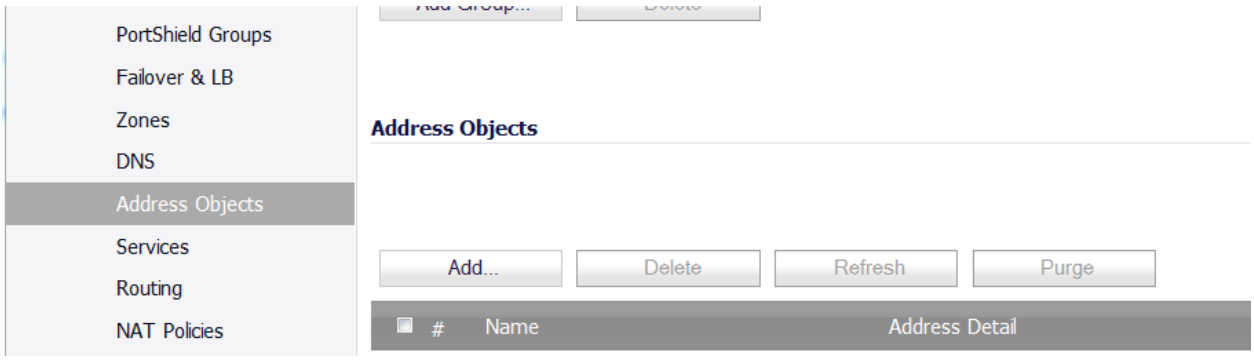
General outline and suggestions

1) Assign/ configure local static IP address in your kiosk/ barcode computer.

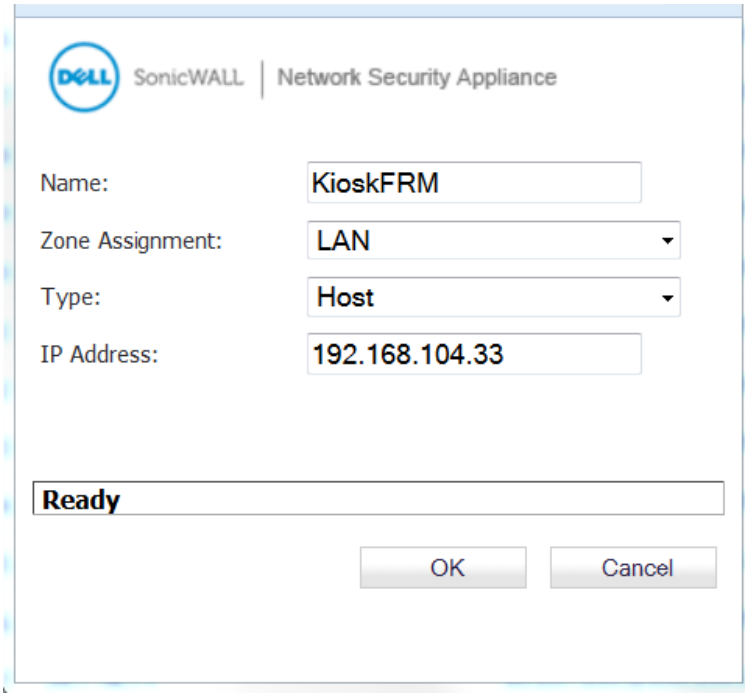
2) In SonicWALL navigate to **Network → Address Objects**



3) Click **Add** under Address Objects to create new Address Object

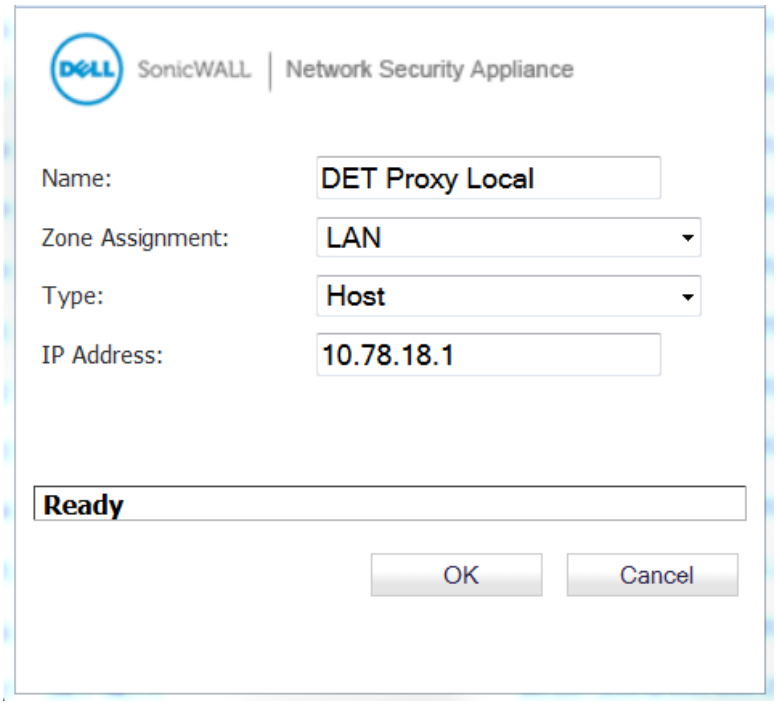


4) A window will pop up. The first **Address Object** we create will be for the **Kiosk** itself, referencing the Static IP created in step 1. Zone Assignment **LAN**, **Type Host**



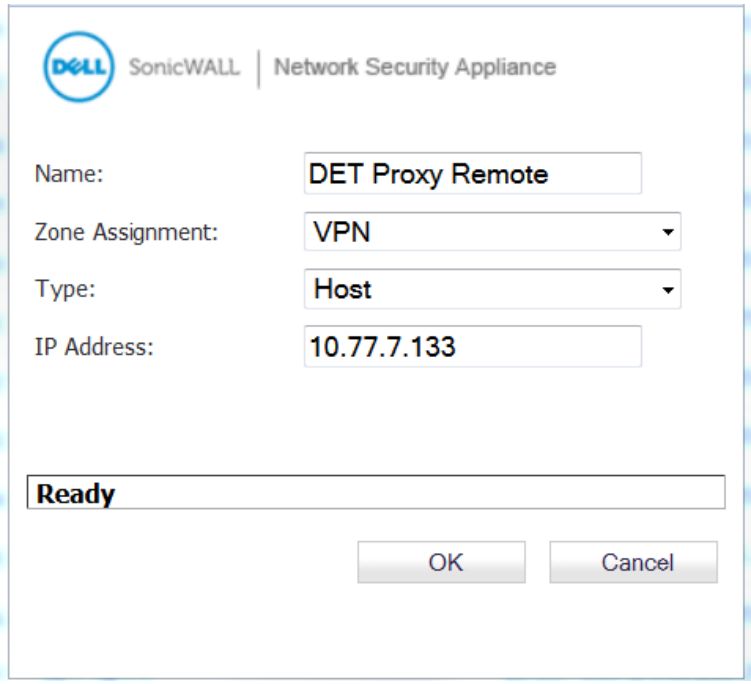
5) Create a 2nd **Address Object**. This is for the **Local Proxy**. This address is provided by DET.

Zone Assignment **LAN**, **Type Host**

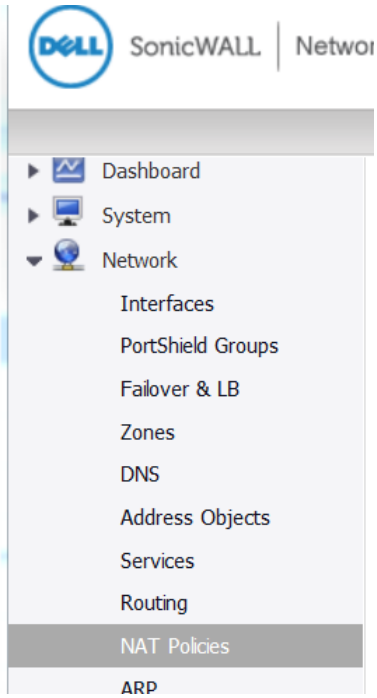


6) Create a 3rd **Address Object**. This is for the **Remote Proxy**. This address is provided by DET.

Zone Assignment **VPN**, **Type Host**



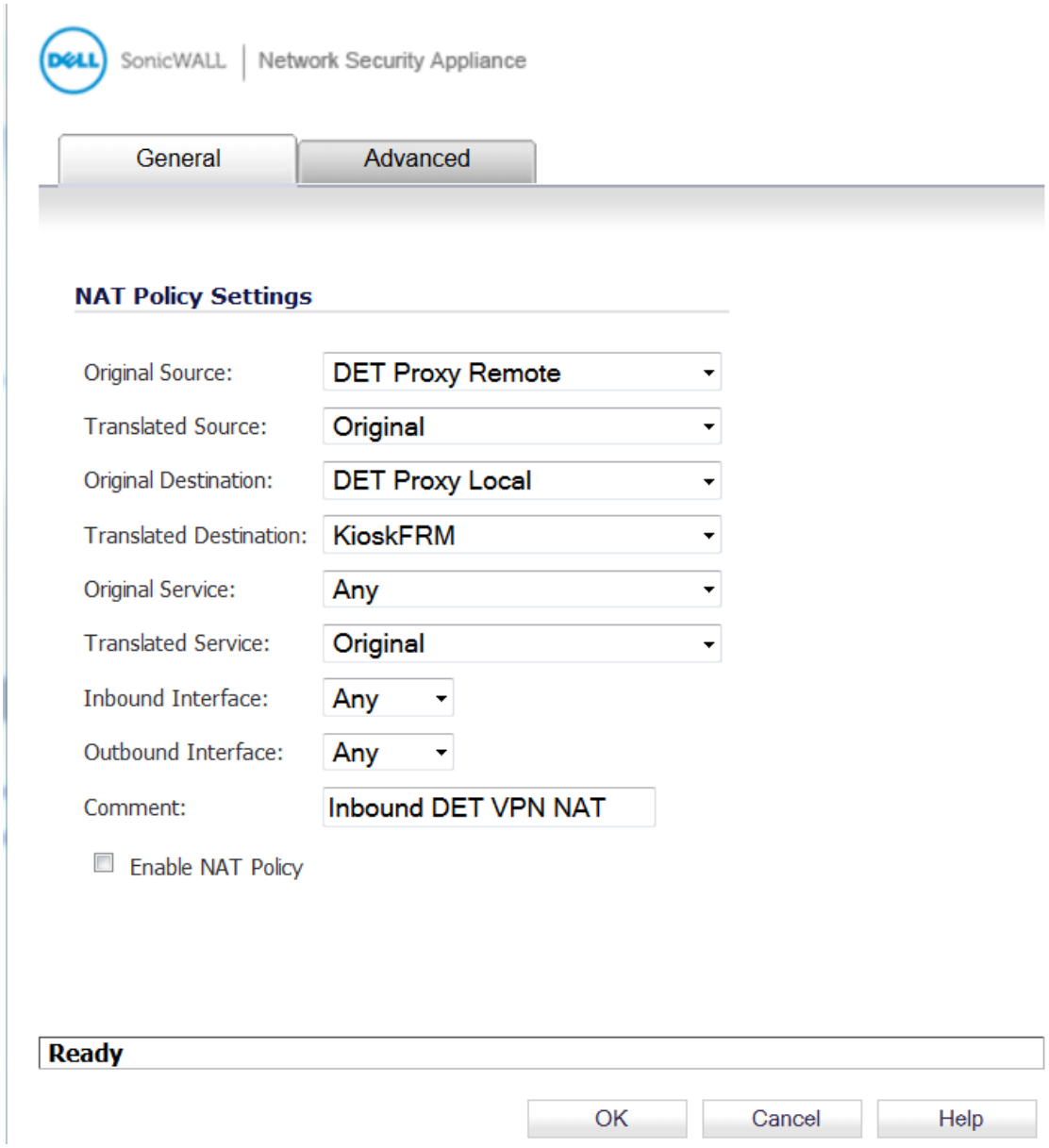
7) Next we go to **Network → NAT Policies**



8) Under **NAT Policies** click **Add**. Here we create the **Inbound VPN NAT Policy**.

Leave **Enable NAT Policy unchecked** for now. We will enable it later.

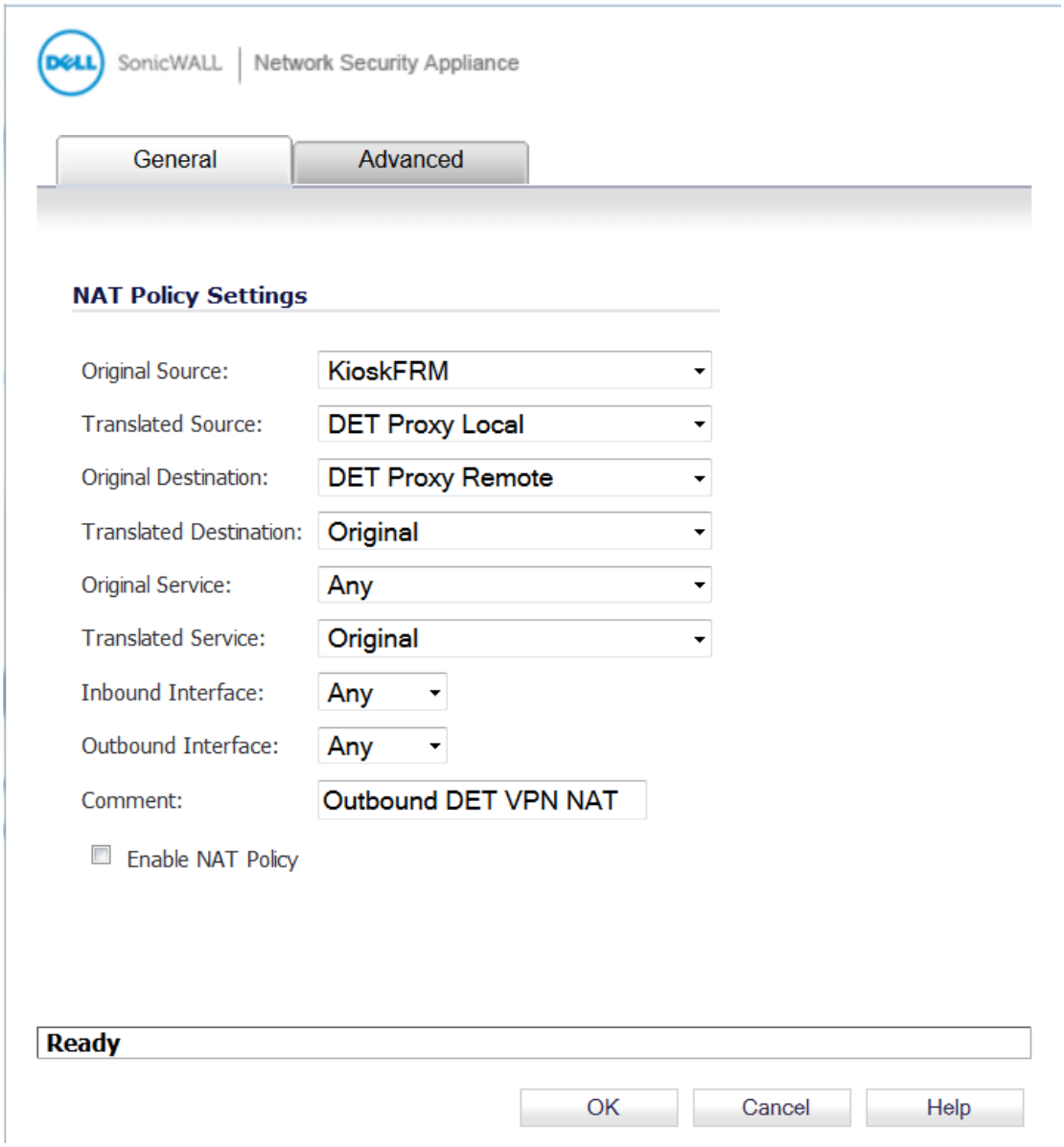
Notice the 3 Address Objects we created in steps 4, 5, 6.



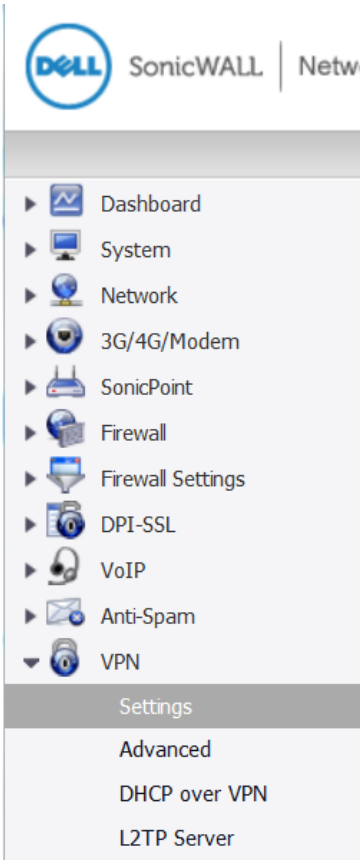
9) Under **NAT Policies**, click **Add** again. Here we create the **Outbound VPN NAT Policy**.

Leave **Enable NAT Policy unchecked** for now. We will enable it later.

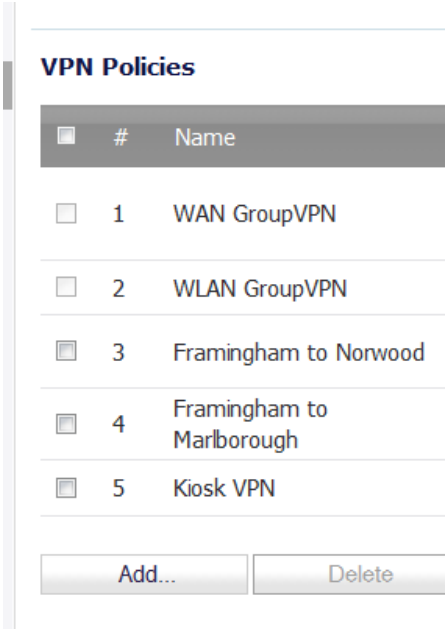
Again, notice the 3 Address Objects we created in steps 4, 5, 6.



10) Now navigate to **VPN → Settings**

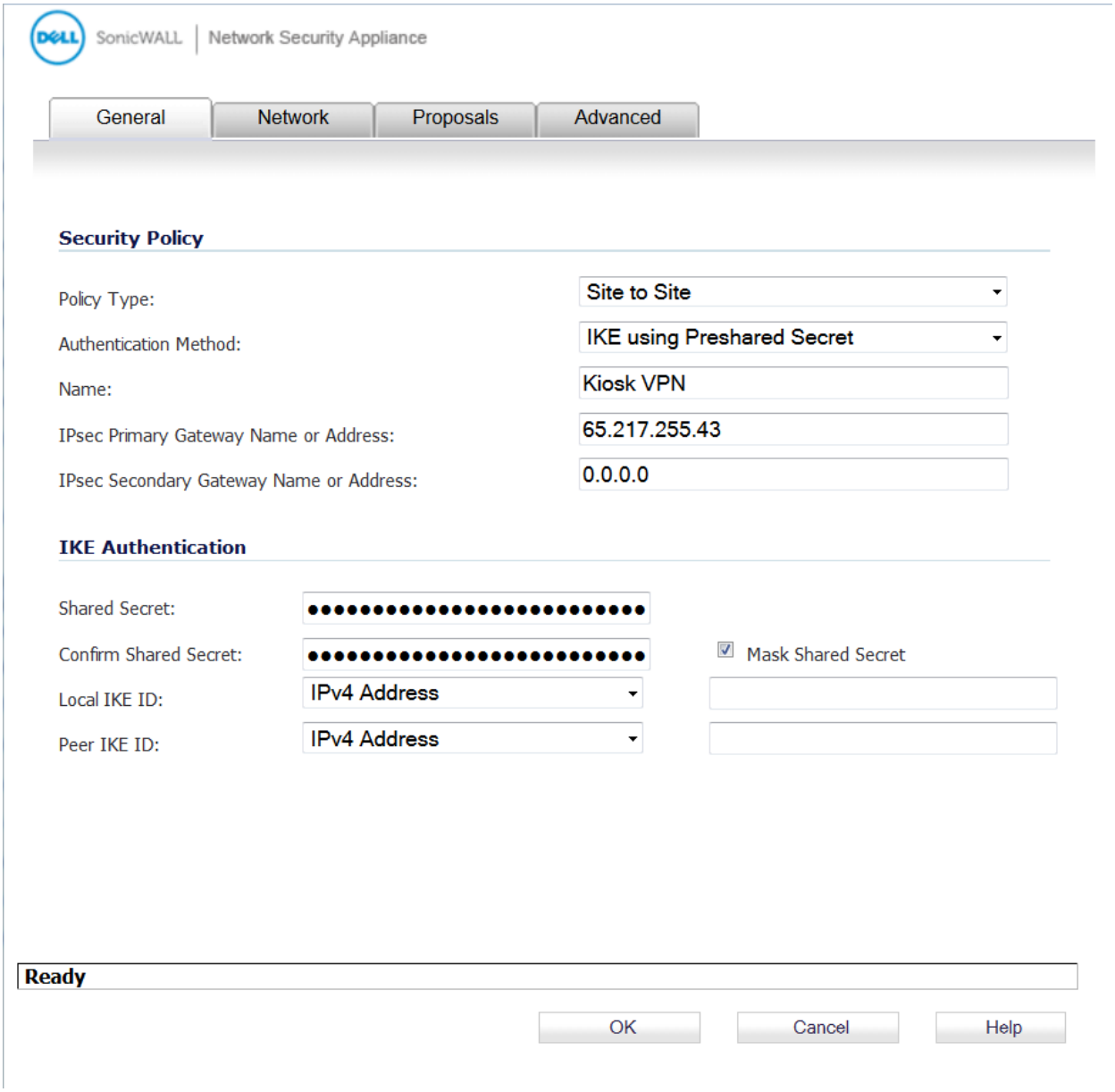


11) Under **VPN Policies** click **Add**

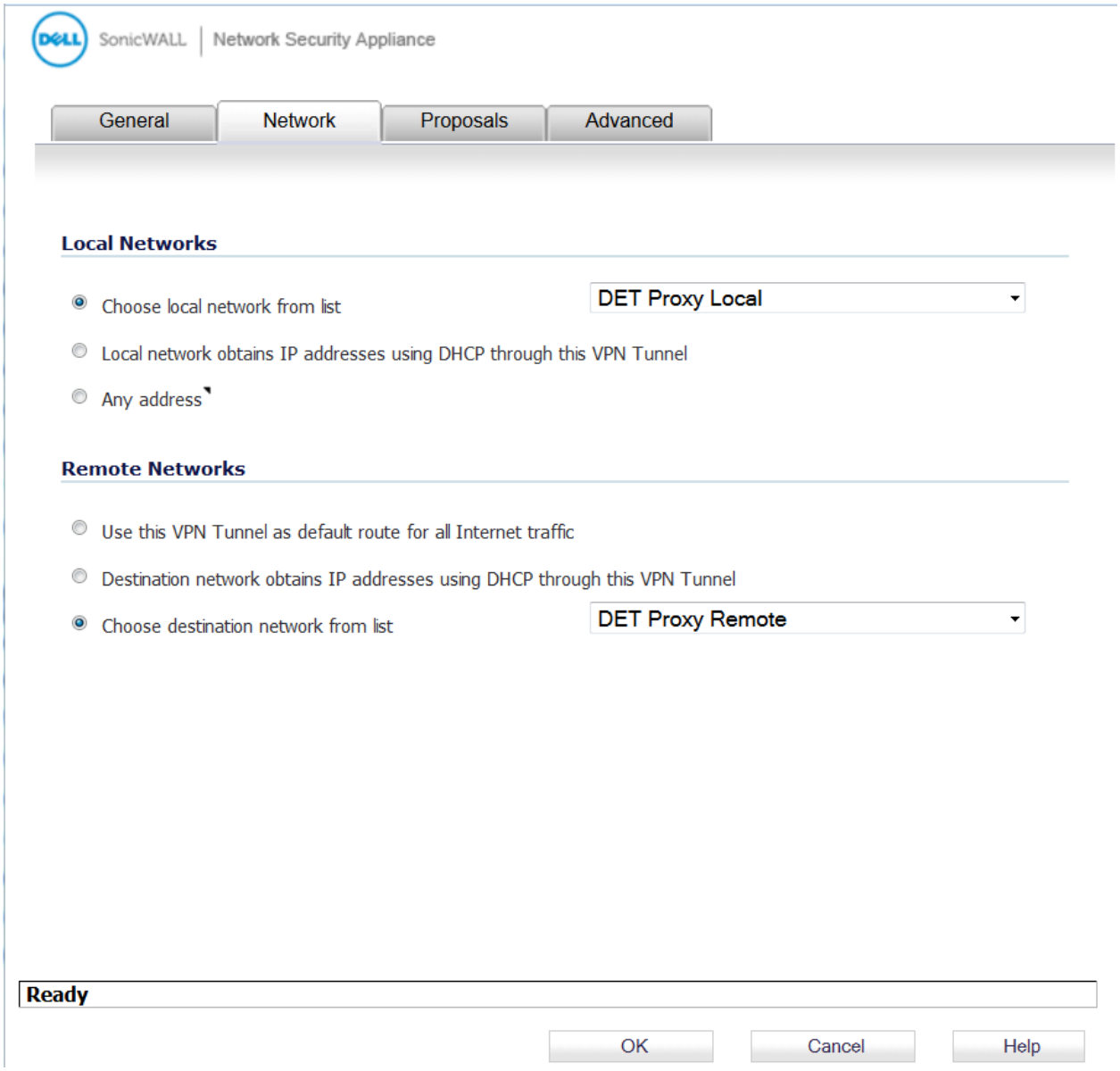


12a) This is the **General** tab where you create the **VPN Policy**. Note, **65.217.255.43** is the Peer IP Address provided by DET which will be the IPsec Primary Gateway.

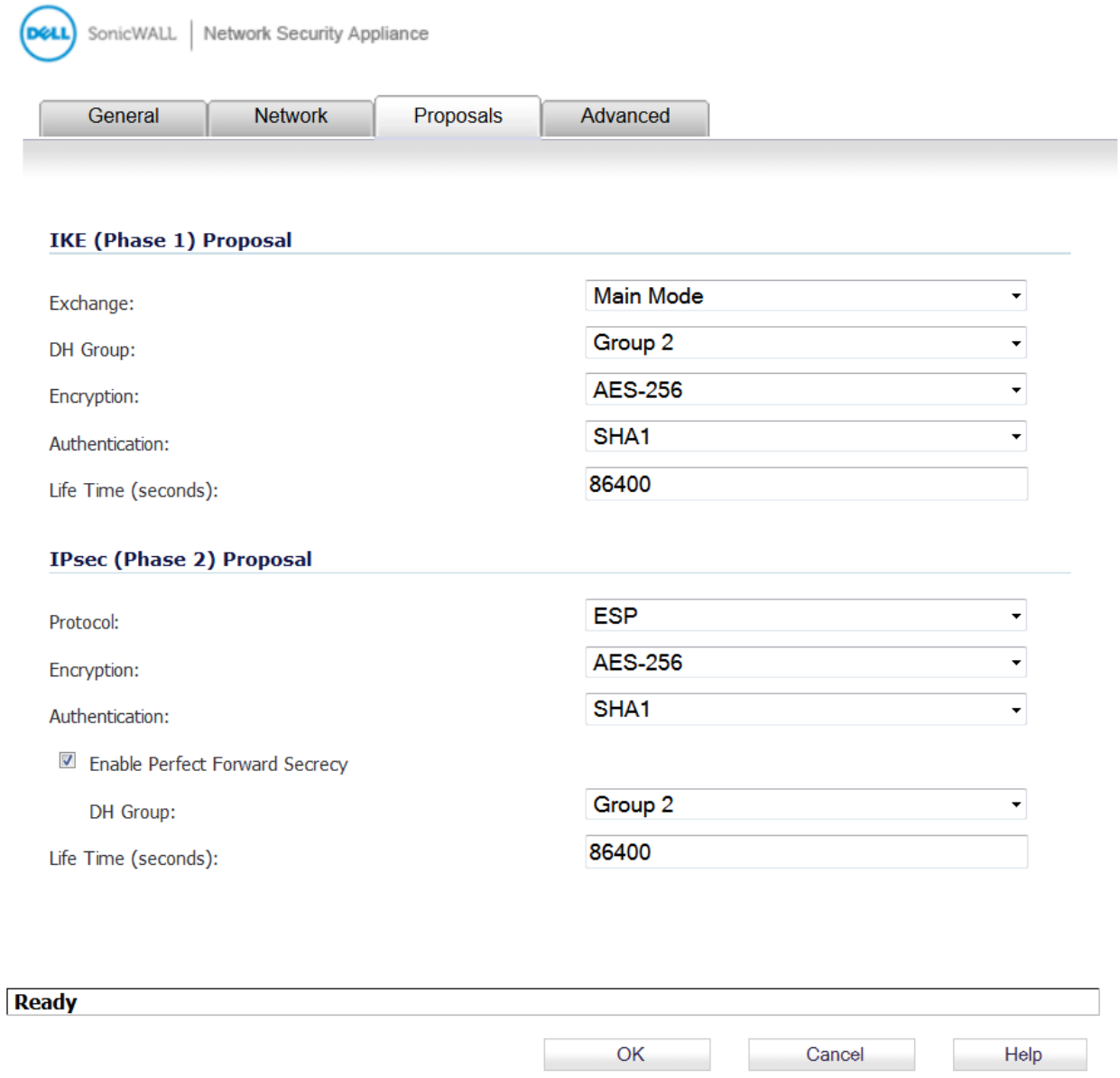
The IKE Authentication **Shared Secret is provided by DET** and <u>not</u> included in this document.



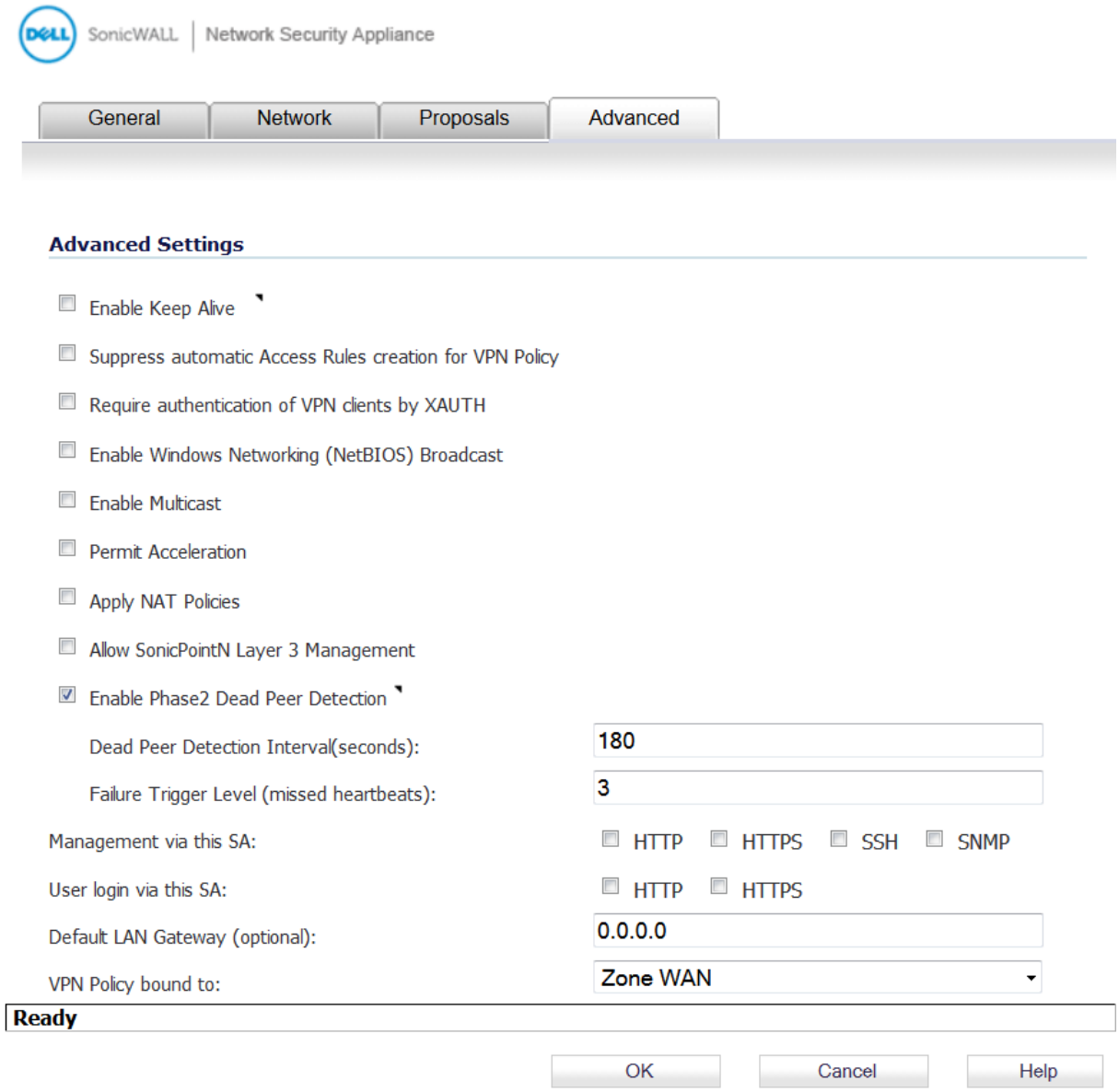
12b) This is the **Network** tab. Notice the Local Networks and Remote Networks are given the Address Objects we created in steps 5 and 6.



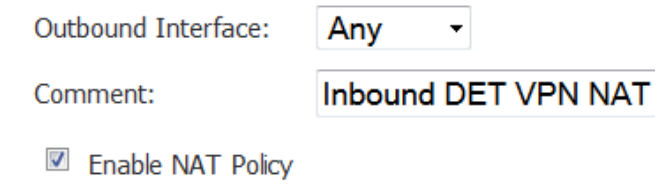
12c) This is the **Proposals** tab. The settings pictured below at time of configuration are correct.

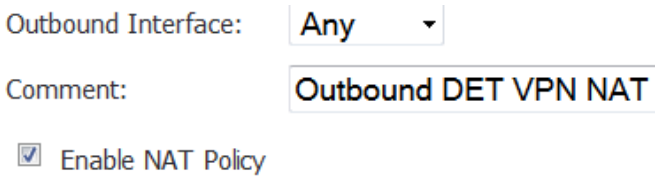


12d) This is the **Advanced** tab. Notice **keep alive is unchecked**, and to my knowledge not required.



13) Go to **Network → NAT Policies** and **enable the NAT Policies** we created in steps 8 and 9





14a) **Testing to see if Tunnel was configured correctly**

First go log onto kiosk / barcode computer we configured in step 1.

Open up a command prompt and **run a continuous ping to DET Proxy Remote**.

If the tunnel is established you should get replies:

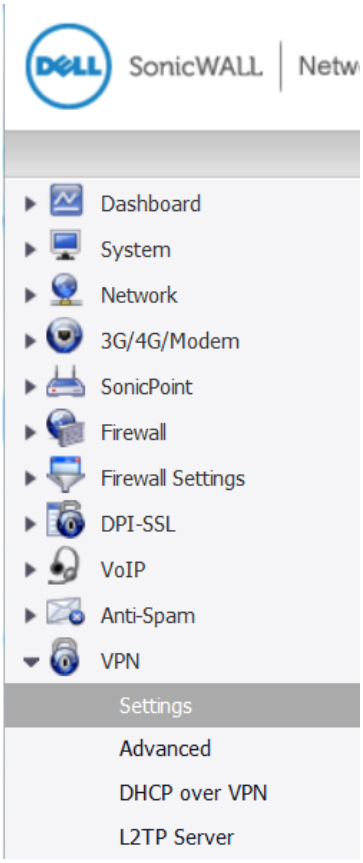
```
C:\Users\Administrator>ping 10.77.7.133 -t

Pinging 10.77.7.133 with 32 bytes of data:
Reply from 10.77.7.133: bytes=32 time=31ms TTL=126
Reply from 10.77.7.133: bytes=32 time=26ms TTL=126
Reply from 10.77.7.133: bytes=32 time=32ms TTL=126
Reply from 10.77.7.133: bytes=32 time=29ms TTL=126
Reply from 10.77.7.133: bytes=32 time=28ms TTL=126
Reply from 10.77.7.133: bytes=32 time=27ms TTL=126
Reply from 10.77.7.133: bytes=32 time=29ms TTL=126
Reply from 10.77.7.133: bytes=32 time=27ms TTL=126
Reply from 10.77.7.133: bytes=32 time=30ms TTL=126
Reply from 10.77.7.133: bytes=32 time=30ms TTL=126
Reply from 10.77.7.133: bytes=32 time=40ms TTL=126
Reply from 10.77.7.133: bytes=32 time=33ms TTL=126
Reply from 10.77.7.133: bytes=32 time=30ms TTL=126
Reply from 10.77.7.133: bytes=32 time=32ms TTL=126
Reply from 10.77.7.133: bytes=32 time=30ms TTL=126
Reply from 10.77.7.133: bytes=32 time=27ms TTL=126
Reply from 10.77.7.133: bytes=32 time=26ms TTL=126
Reply from 10.77.7.133: bytes=32 time=28ms TTL=126
Reply from 10.77.7.133: bytes=32 time=29ms TTL=126
Reply from 10.77.7.133: bytes=32 time=28ms TTL=126
Reply from 10.77.7.133: bytes=32 time=30ms TTL=126

Ping statistics for 10.77.7.133:
    Packets: Sent = 21, Received = 21, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 40ms, Average = 29ms
```

14b) **Testing to see if Tunnel was configured correctly**

Another indication the tunnel is configured correctly is to go back to **VPN → Settings**



See if there is a **green light** indicating the tunnel you created in step 12 is active. Keep ping from the kiosk continuous during this testing.

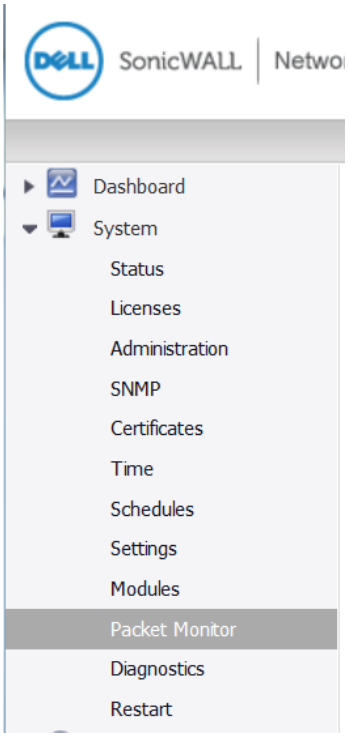
Hint: You may have to **uncheck and check the 'enable' box** pictured above to connect the first time.

Part 2

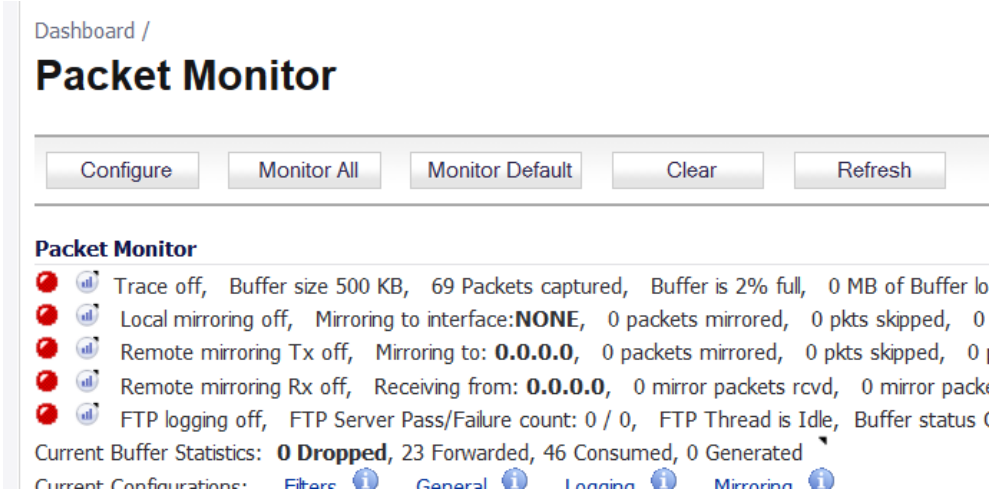
Setting up Packet Monitor to help troubleshoot connection problems

Basic setup

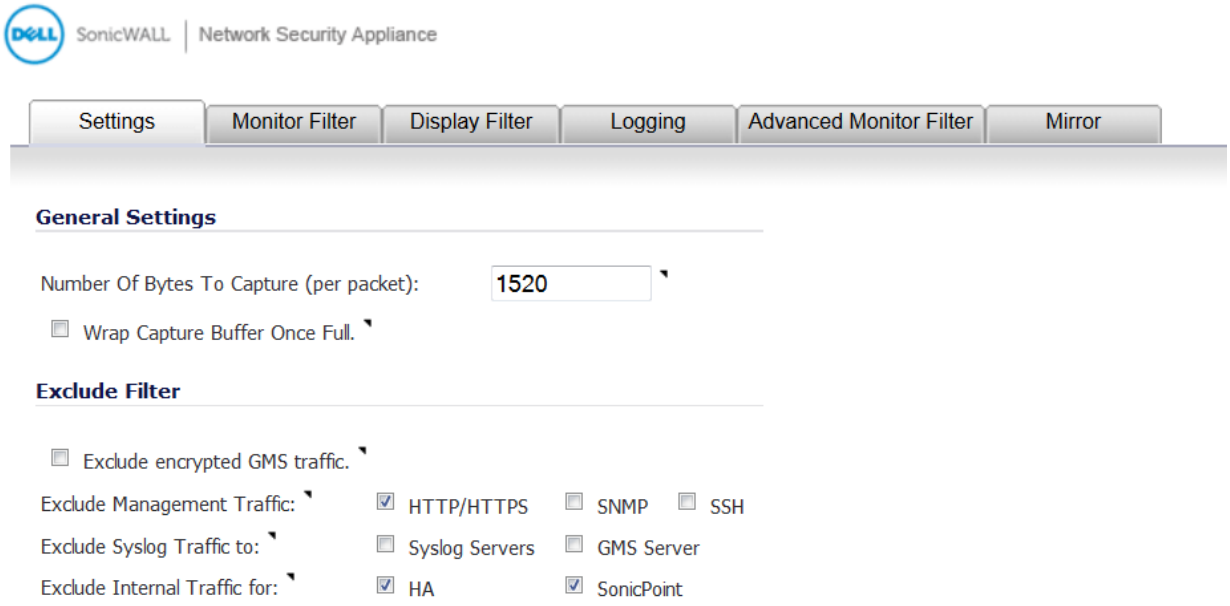
1) In SonicWALL navigate to **System → Packet Monitor**



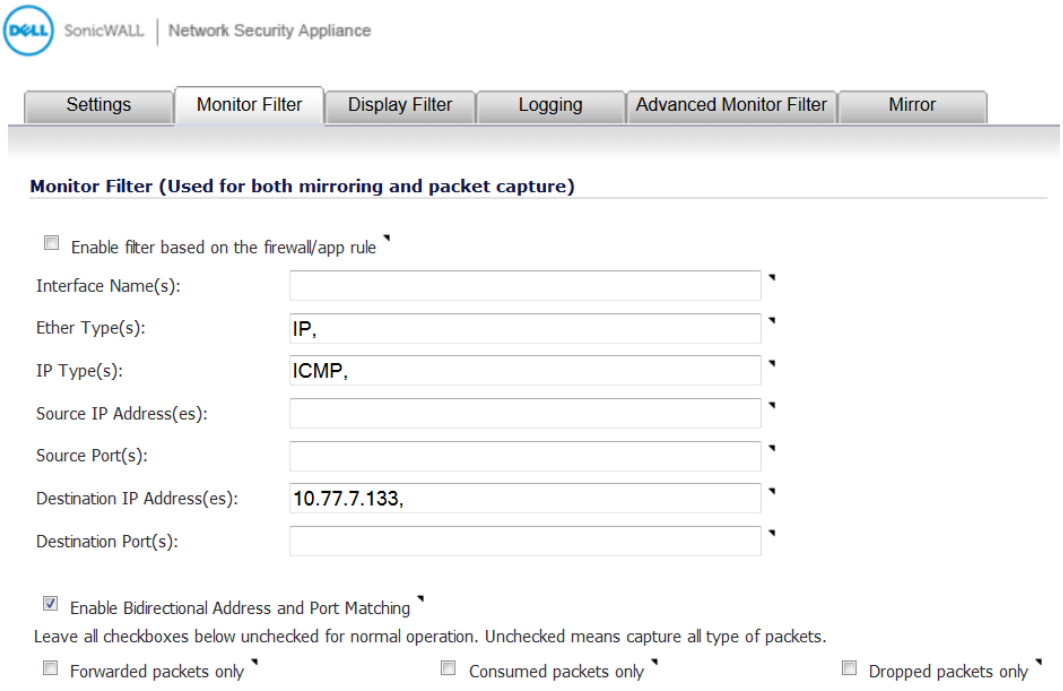
2) Click **Configure**



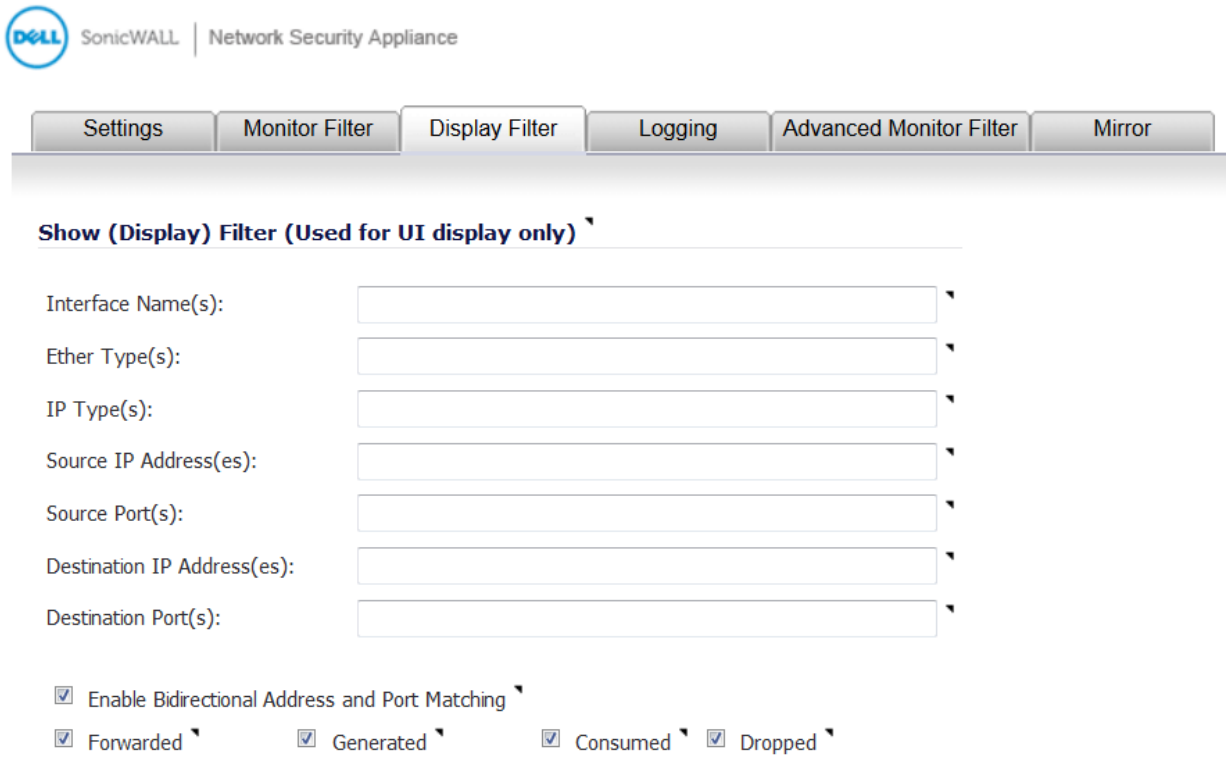
3a) **Packet Monitor, Settings** tab



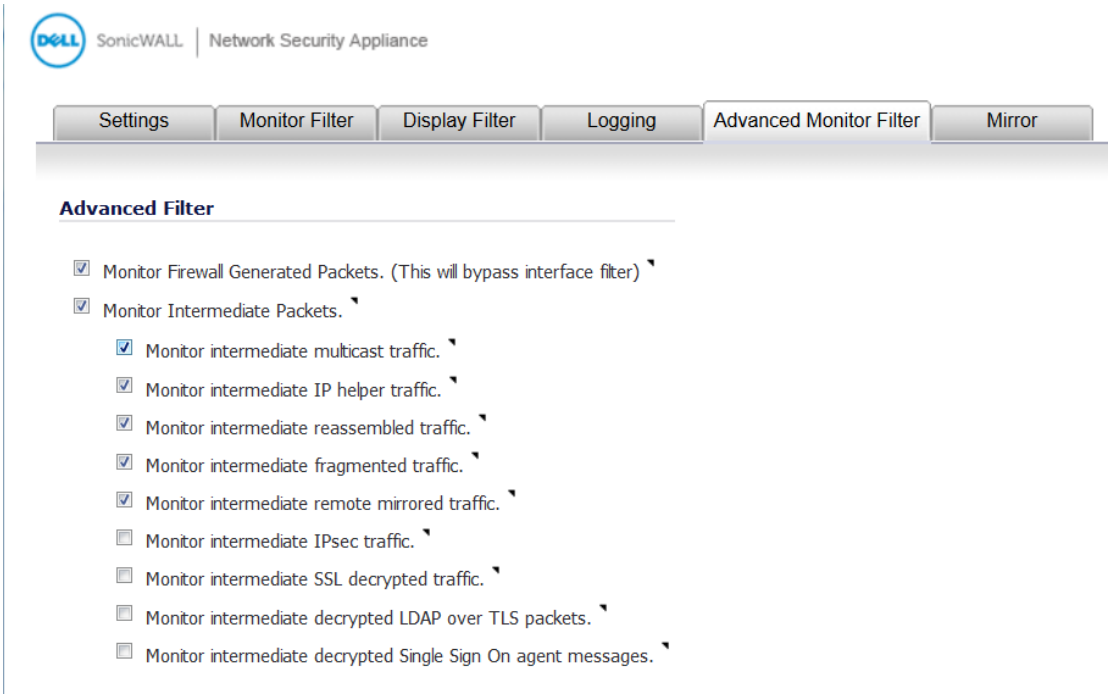
3b) **Packet Monitor, Monitor Filter** tab



3c) **Packet Monitor, Display Filter** tab



3d) **Packet Monitor, Advanced Monitor Filter** tab



4) Start **continuous ping to 10.77.7.133 from kiosk/barcode computer**

(you will not get reply if there is a connection problem)

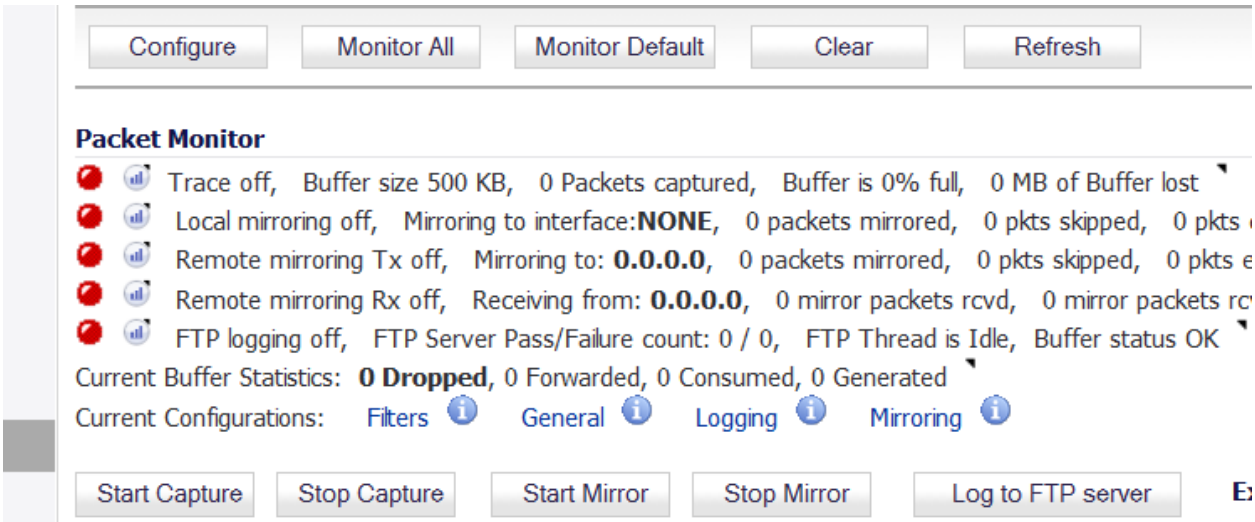
```
C:\Users\Administrator>ping 10.77.7.133 -t

Pinging 10.77.7.133 with 32 bytes of data:
Reply from 10.77.7.133: bytes=32 time=31ms TTL=126
Reply from 10.77.7.133: bytes=32 time=26ms TTL=126
Reply from 10.77.7.133: bytes=32 time=32ms TTL=126
Reply from 10.77.7.133: bytes=32 time=29ms TTL=126
Reply from 10.77.7.133: bytes=32 time=28ms TTL=126
Reply from 10.77.7.133: bytes=32 time=27ms TTL=126
Reply from 10.77.7.133: bytes=32 time=29ms TTL=126
Reply from 10.77.7.133: bytes=32 time=27ms TTL=126
Reply from 10.77.7.133: bytes=32 time=30ms TTL=126
Reply from 10.77.7.133: bytes=32 time=30ms TTL=126
Reply from 10.77.7.133: bytes=32 time=40ms TTL=126
Reply from 10.77.7.133: bytes=32 time=33ms TTL=126
Reply from 10.77.7.133: bytes=32 time=30ms TTL=126
Reply from 10.77.7.133: bytes=32 time=32ms TTL=126
Reply from 10.77.7.133: bytes=32 time=30ms TTL=126
Reply from 10.77.7.133: bytes=32 time=27ms TTL=126
Reply from 10.77.7.133: bytes=32 time=26ms TTL=126
Reply from 10.77.7.133: bytes=32 time=28ms TTL=126
Reply from 10.77.7.133: bytes=32 time=29ms TTL=126
Reply from 10.77.7.133: bytes=32 time=28ms TTL=126
Reply from 10.77.7.133: bytes=32 time=30ms TTL=126

Ping statistics for 10.77.7.133:
    Packets: Sent = 21, Received = 21, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 40ms, Average = 29ms
```

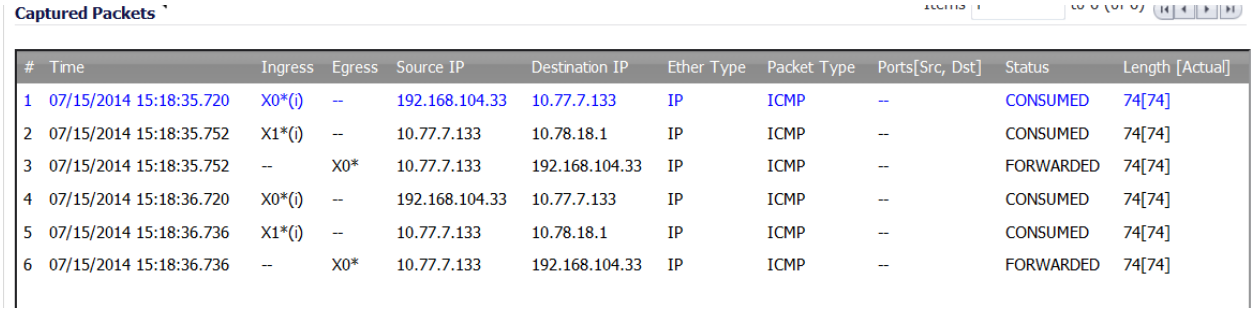
5) Back to **System → Packet Monitor** click **Start Capture**

(hint: you may have to **click Clear first** if the buffer is already full)



6) You will see something like this if the capture is working.

This is the traffic I see when the tunnel is active and there is a response to ping



Captured Packets

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	07/15/2014 15:18:35.720	X0*(i)	--	192.168.104.33	10.77.7.133	IP	ICMP	--	CONSUMED	74[74]
2	07/15/2014 15:18:35.752	X1*(i)	--	10.77.7.133	10.78.18.1	IP	ICMP	--	CONSUMED	74[74]
3	07/15/2014 15:18:35.752	--	X0*	10.77.7.133	192.168.104.33	IP	ICMP	--	FORWARDED	74[74]
4	07/15/2014 15:18:36.720	X0*(i)	--	192.168.104.33	10.77.7.133	IP	ICMP	--	CONSUMED	74[74]
5	07/15/2014 15:18:36.736	X1*(i)	--	10.77.7.133	10.78.18.1	IP	ICMP	--	CONSUMED	74[74]
6	07/15/2014 15:18:36.736	--	X0*	10.77.7.133	192.168.104.33	IP	ICMP	--	FORWARDED	74[74]

Part 3

VBS script and batch file to ensure tunnel activity

These simple files work together to send a single ping (IMCP) every 10 minutes over the IPsec VPN from your kiosk or barcode computer to ensure the tunnel remains open and active all day

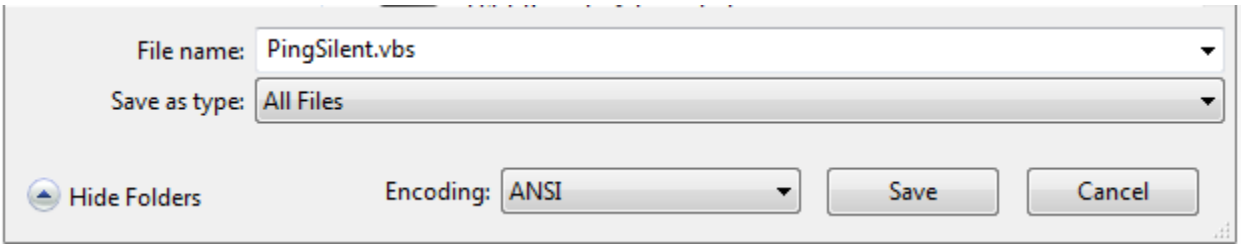
1) Log into your kiosk / barcode computer configured in step 1 of this document. Two files need to be created. Choose a location such as the local administrator desktop, and note the path, such as,

C:\Users\Administrator\Desktop

2) Open up notepad and paste the following. Change the path as required:

```
Set objShell = WScript.CreateObject("WScript.Shell")
objShell.Run("C:\Users\Administrator\Desktop\AutoPing.bat"), 0, True
```

Save As: **PingSilent.vbs** in the folder location you have chosen

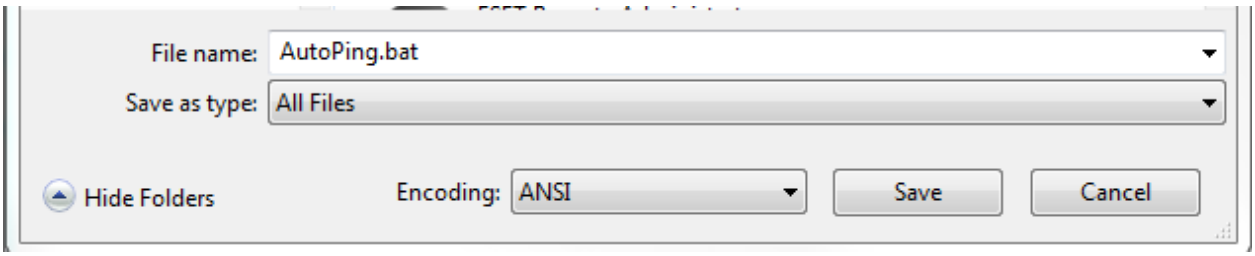


Be sure to change '**Save as type**' from Text Document (*.txt) to **All Files**.

3) Open up notepad once more and paste the following:

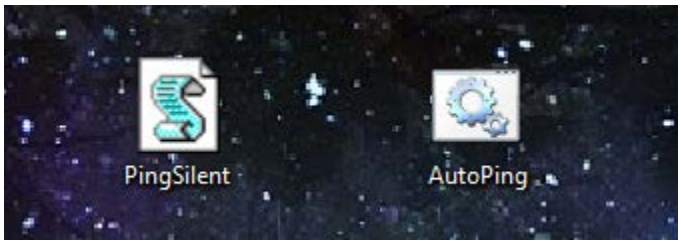
```
:begin
ping -n 1 10.77.7.133
PING 1.1.1.1 -n 1 -w 600000 >NUL
goto begin
```

Save As: **AutoPing.bat** in the folder location you have chosen



Again, choose **All Files** as the file type.

4) If you created these files correctly, the icons should look like this:

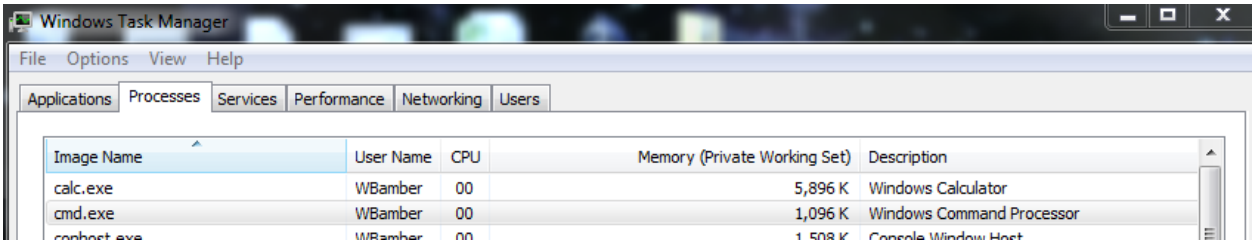


AutoPing.bat launches **CMD to ping 10.77.7.133 once every 10 minutes** or 600000 ms, and will run **continuously**. If you double click AutoPing.bat, a CMD shell will pop up and will begin the loop. However, we do not want a CMD shell to pop up on the screen our customers interact with, or be visible on the taskbar.

PingSilent.vbs opens **AutoPing.bat** and causes **cmd.exe to run silently**. Nothing pops up or is indicated on the taskbar.

5a) Simple way to verify it is running:

Double click **PingSilent.vbs** on your kiosk computer
Open up **Task Manager → Processes**
Verify **cmd.exe** is running:

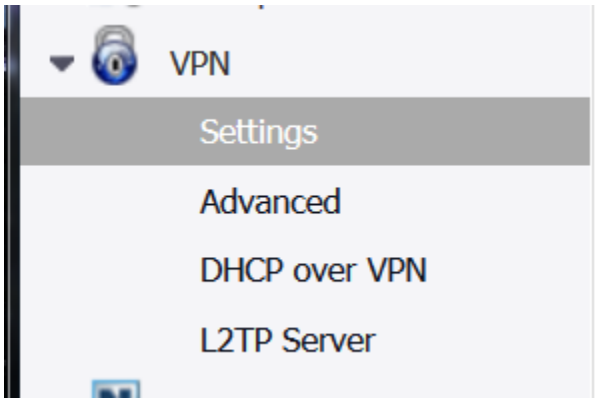


5b) Verify tunnel can be triggered open, and traffic is flowing

1. Open up **Task Manager → Processes** on your kiosk /barcode computer, select **cmd.exe** (if still running) and click **End Process**.

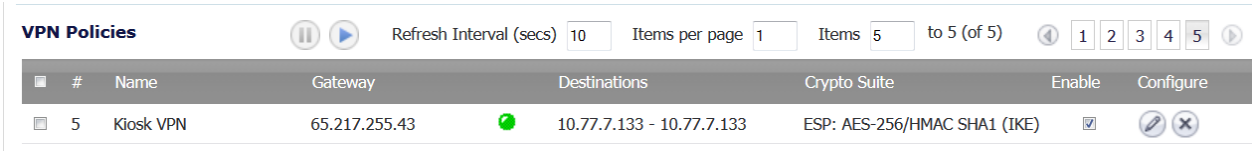
2. Log into your SonicWALL appliance

3. Navigate to **VPN → Settings**:



4. **Uncheck** the 'enable box' for your DET IPsec VPN, count to 10 **and recheck** same box.

The tunnel will be enabled but closed.



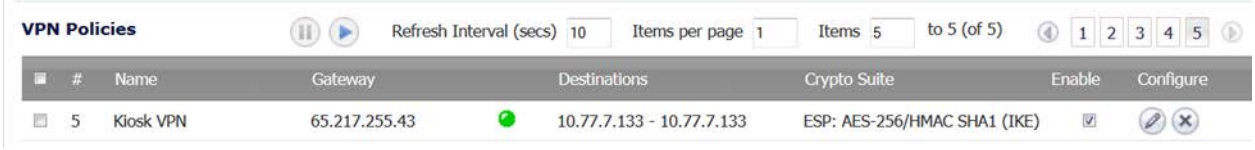
(Please note, the green light will be **gray** if you successfully closed the tunnel)

5. Navigate to **System → Packet Monitor**

6. Filter Packet Monitor for **bidirectional ICMP** Traffic to **10.77.7.133** & **Start Capture**
(If you need tips on how to do this please refer to Part 2 of this document)

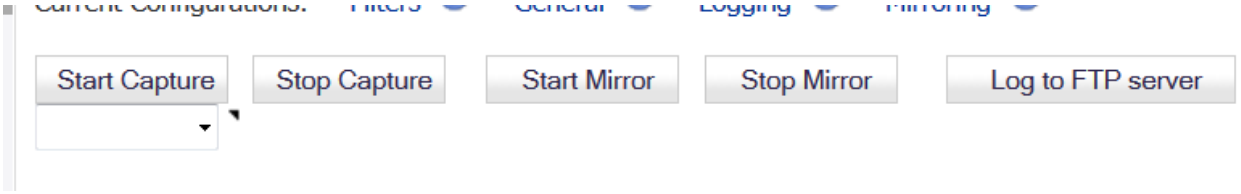
7. On your Kiosk computer double click on **PingSilent.vbs**
(This should open the tunnel)

8. Return to **VPN → Settings** on your SonicWALL
Verify the IPsec Tunnel is now open ("**green light**")



9. Navigate back to **System → Packet Monitor**

Click **Stop Capture**.



10. If everything goes as expected, you will see **ICMP** traffic.

Captured Packets

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	08/21/2014 11:25:39.352	X0*(i)	--	192.168.104.33	10.77.7.133	IP	ICMP	--	CONSUMED	74[74]
2	08/21/2014 11:25:39.368	X1*(i)	--	10.77.7.133	10.78.18.1	IP	ICMP	--	CONSUMED	74[74]
3	08/21/2014 11:25:39.368	--	X0*	10.77.7.133	192.168.104.33	IP	ICMP	--	FORWARDED	74[74]

note: The first 'ping' always times out on a closed tunnel, but it **will open the tunnel** in the process. This is its purpose. I call it a 'sacrificial ping'!

11. We suggest you set **PingSilent.vbs** to either run at OS startup or to run in the morning with Task Scheduler. This way no user interaction is required.

It will run continuously until forced to stop.

William Bamber 7/15/2014 ||| Rev B - 8/25/2014

wbamber@etrcc.com