

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

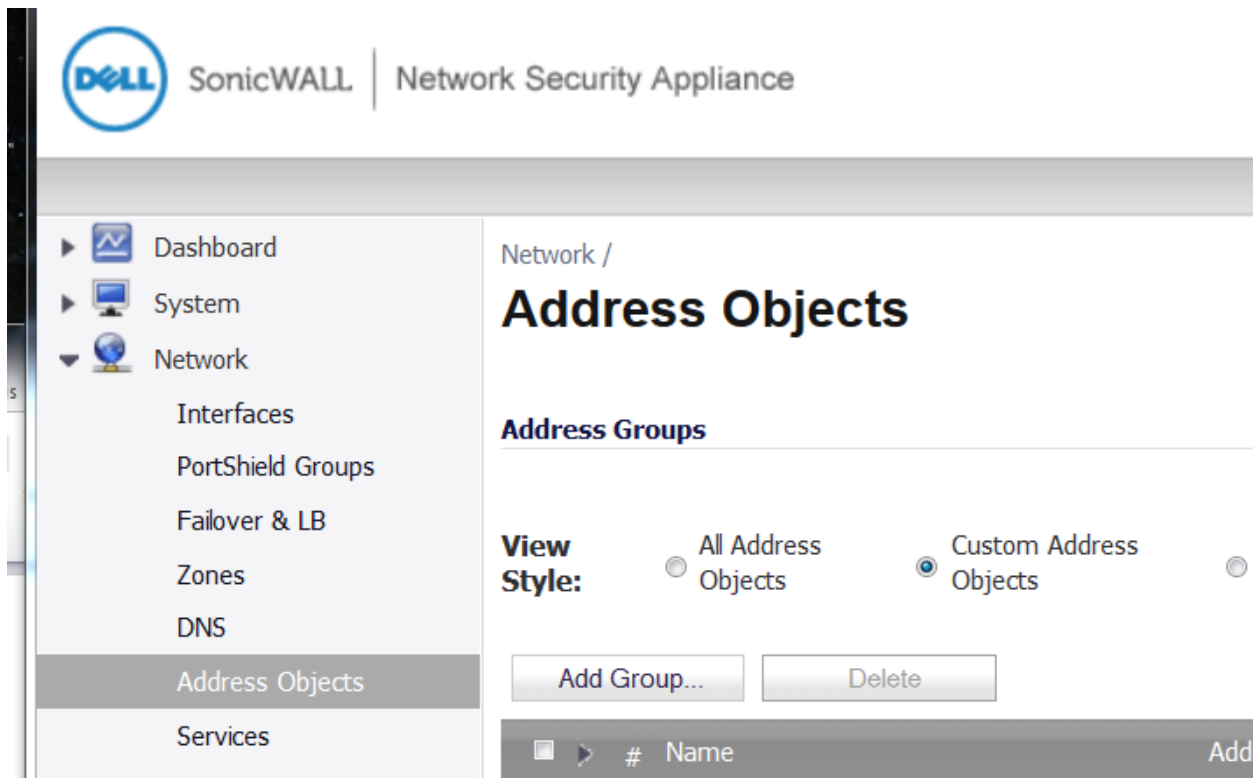
Rev B | 8/25/14

Part 1

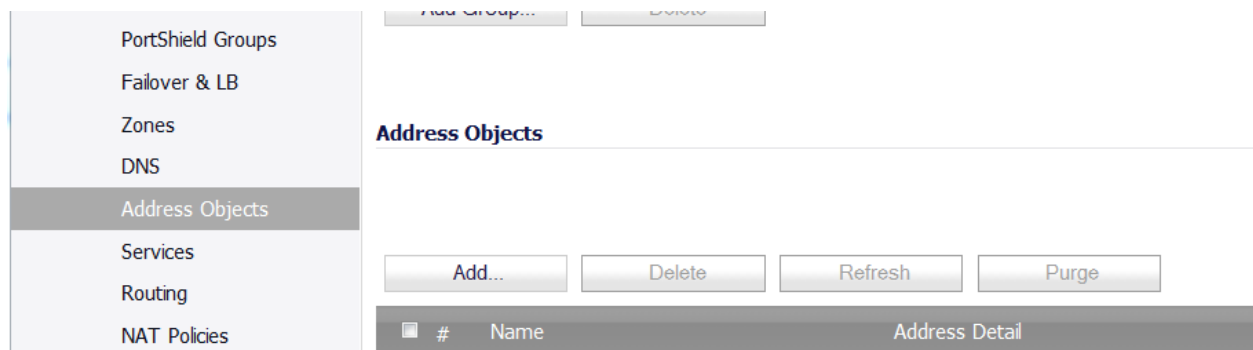
Configuring SonicWALL NSA 250M for IPsec VPN Tunnel to DET ASA

General outline and suggestions

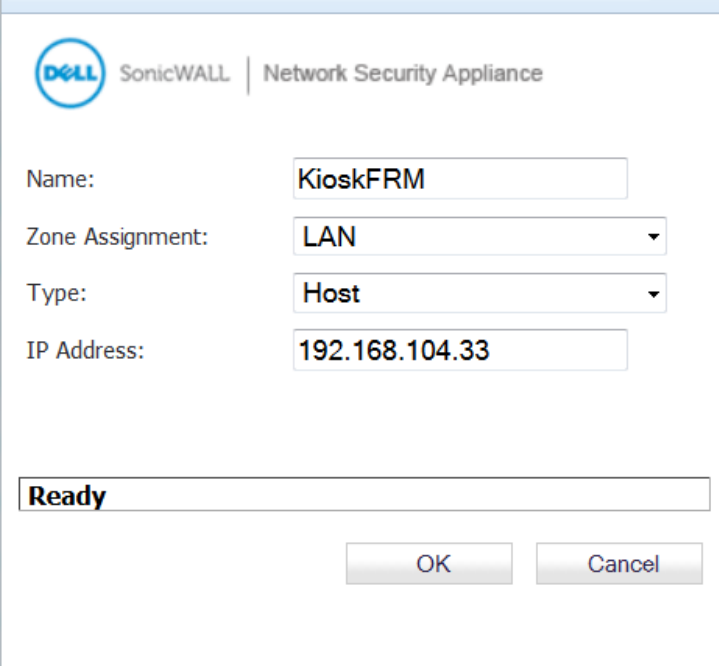
- 1) Assign/ configure local static IP address in your kiosk/ barcode computer.
- 2) In SonicWALL navigate to **Network → Address Objects**



- 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**



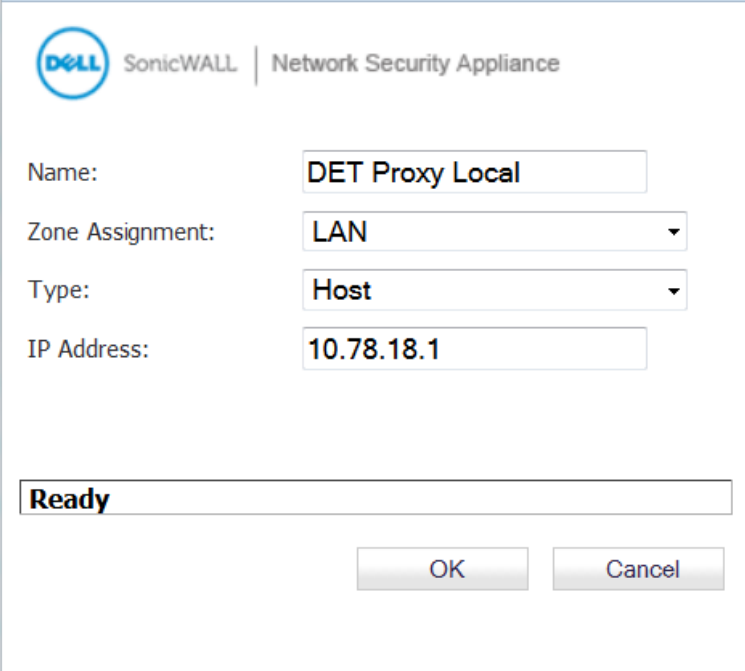
The image shows a configuration window from the SonicWALL Network Security Appliance. It contains the following fields and values:

Field	Value
Name:	KioskFRM
Zone Assignment:	LAN
Type:	Host
IP Address:	192.168.104.33

At the bottom, there is a status bar that says "Ready" and two buttons: "OK" and "Cancel".

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

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



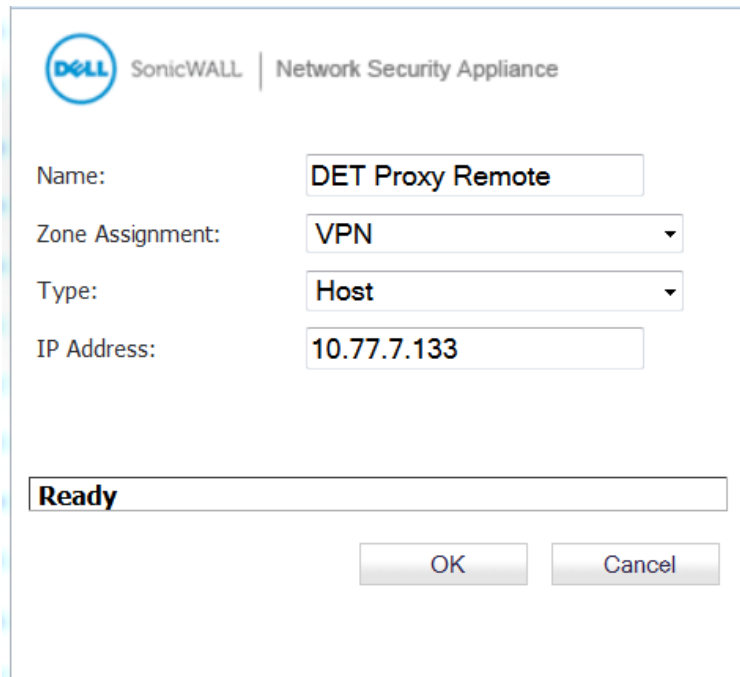
The image shows a configuration window from the SonicWALL Network Security Appliance. It contains the following fields and values:

Field	Value
Name:	DET Proxy Local
Zone Assignment:	LAN
Type:	Host
IP Address:	10.78.18.1

At the bottom, there is a status bar that says "Ready" and two buttons: "OK" and "Cancel".

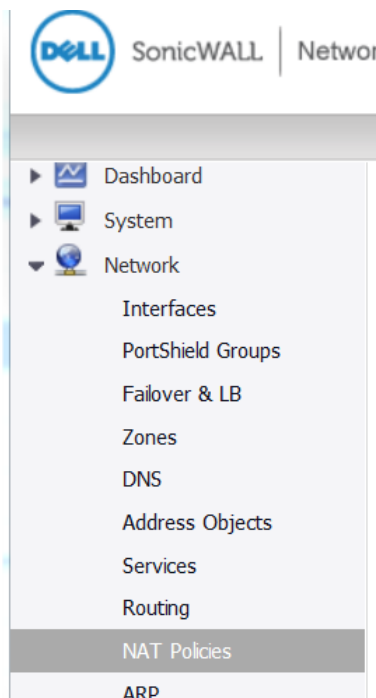
6) Create a 3rd **Address Object**. This is for the **Remote Proxy**. This address is provided by DET.

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



The image shows a configuration window for a SonicWALL Network Security Appliance. The window has a title bar with the Dell SonicWALL logo and the text "Network Security Appliance". Inside the window, there are four labeled text input fields: "Name:" with the value "DET Proxy Remote", "Zone Assignment:" with a dropdown menu showing "VPN", "Type:" with a dropdown menu showing "Host", and "IP Address:" with the value "10.77.7.133". Below these fields is a status bar that says "Ready". At the bottom right of the window are two buttons: "OK" and "Cancel".

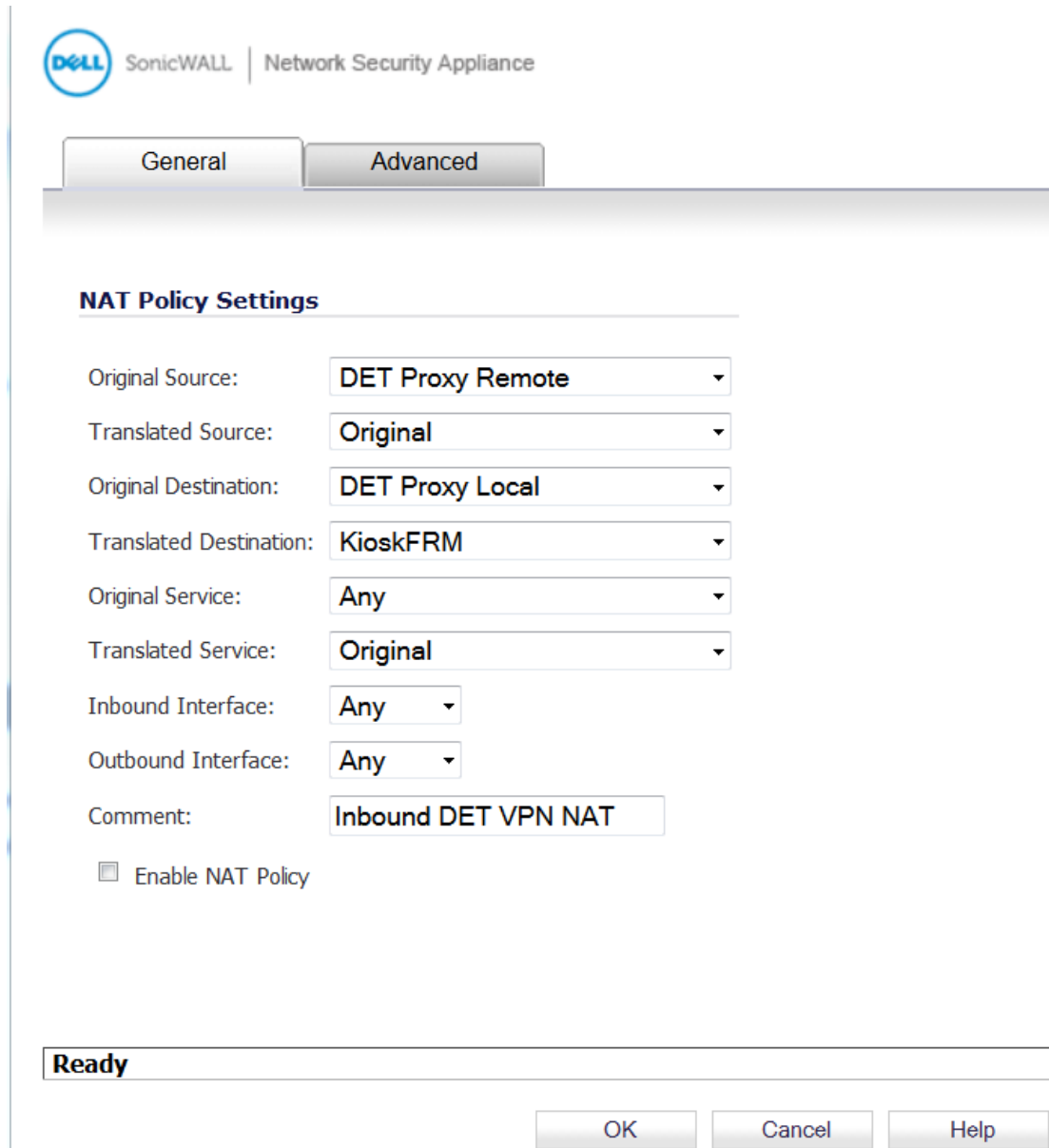
7) Next we go to **Network** → **NAT Policies**



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.



The screenshot shows the SonicWALL Network Security Appliance interface. At the top, there is a header with the Dell logo, 'SonicWALL', and 'Network Security Appliance'. Below this, there are two tabs: 'General' (selected) and 'Advanced'. The main section is titled 'NAT Policy Settings'. It contains several configuration fields, each with a label and a dropdown menu or text box:

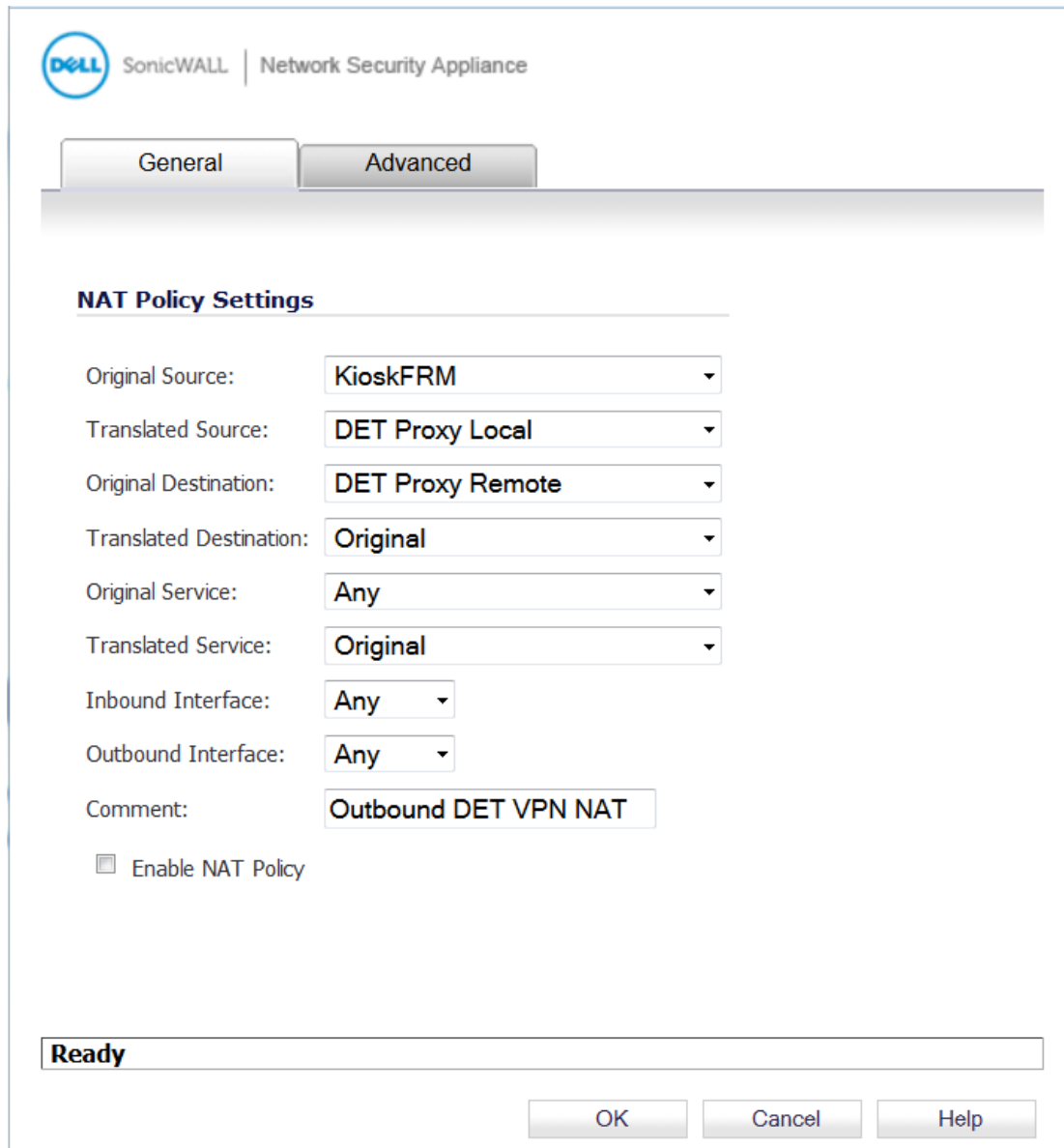
- Original Source: DET Proxy Remote
- Translated Source: Original
- Original Destination: DET Proxy Local
- Translated Destination: KioskFRM
- Original Service: Any
- Translated Service: Original
- Inbound Interface: Any
- Outbound Interface: Any
- Comment: Inbound DET VPN NAT

Below these fields is a checkbox labeled 'Enable NAT Policy', which is currently unchecked. At the bottom of the dialog, there is a status bar that says 'Ready'. To the right of the status bar are three buttons: 'OK', 'Cancel', and 'Help'.

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.

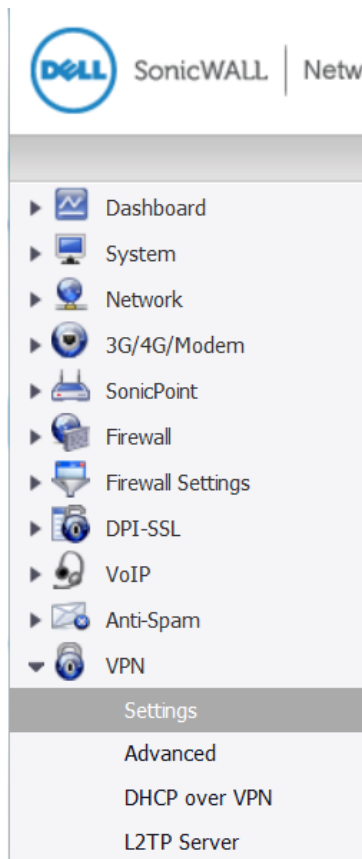


The screenshot shows the 'NAT Policy Settings' dialog box in the SonicWALL Network Security Appliance interface. The 'General' tab is selected. The settings are as follows:

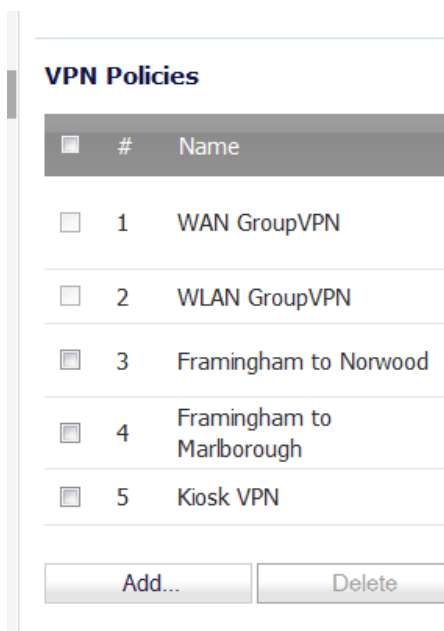
Field	Value
Original Source:	KioskFRM
Translated Source:	DET Proxy Local
Original Destination:	DET Proxy Remote
Translated Destination:	Original
Original Service:	Any
Translated Service:	Original
Inbound Interface:	Any
Outbound Interface:	Any
Comment:	Outbound DET VPN NAT
Enable NAT Policy	<input type="checkbox"/>

At the bottom of the dialog, there is a status bar that says 'Ready' and three buttons: 'OK', 'Cancel', and 'Help'.

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 not included in this document.

 SonicWALL | Network Security Appliance

General

Network

Proposals

Advanced

Security Policy

Policy Type:

Site to Site

Authentication Method:

IKE using Preshared Secret

Name:

Kiosk VPN

IPsec Primary Gateway Name or Address:

65.217.255.43

IPsec Secondary Gateway Name or Address:

0.0.0.0

IKE Authentication

Shared Secret:

.....

Confirm Shared Secret:

.....

Local IKE ID:

IPv4 Address

Peer IKE ID:

IPv4 Address

☒ Mask Shared Secret

Ready

OK

Cancel

Help

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.

The screenshot shows the SonicWALL Network Security Appliance configuration interface. At the top, the Dell logo and 'SonicWALL | Network Security Appliance' are visible. Below this is a tabbed interface with four tabs: 'General', 'Network' (which is selected), 'Proposals', and 'Advanced'. The 'Network' tab is divided into two sections: 'Local Networks' and 'Remote Networks'. In the 'Local Networks' section, there are three radio button options: 'Choose local network from list' (which is selected), 'Local network obtains IP addresses using DHCP through this VPN Tunnel', and 'Any address'. To the right of the selected option is a dropdown menu showing 'DET Proxy Local'. In the 'Remote Networks' section, there are three radio button options: 'Use this VPN Tunnel as default route for all Internet traffic', 'Destination network obtains IP addresses using DHCP through this VPN Tunnel', and 'Choose destination network from list' (which is selected). To the right of the selected option is a dropdown menu showing 'DET Proxy Remote'. At the bottom of the window, there is a status bar that says 'Ready' and three buttons: 'OK', 'Cancel', and 'Help'.

SonicWALL | Network Security Appliance

General **Network** **Proposals** **Advanced**

Local Networks

- ☒ Choose local network from list DET Proxy Local
- ☐ Local network obtains IP addresses using DHCP through this VPN Tunnel
- ☐ Any address


Remote Networks

- ☐ Use this VPN Tunnel as default route for all Internet traffic
- ☐ Destination network obtains IP addresses using DHCP through this VPN Tunnel
- ☒ Choose destination network from list DET Proxy Remote

Ready

OK **Cancel** **Help**

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

 SonicWALL | Network Security Appliance

General

Network

Proposals

Advanced

IKE (Phase 1) Proposal

Exchange:

Main Mode

DH Group:

Group 2

Encryption:

AES-256

Authentication:

SHA1

Life Time (seconds):

86400

IPsec (Phase 2) Proposal

Protocol:

ESP

Encryption:

AES-256

Authentication:

SHA1

☒ Enable Perfect Forward Secrecy

DH Group:

Group 2

Life Time (seconds):

86400


Ready

OK

Cancel

Help

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

 SonicWALL | Network Security Appliance

General

Network

Proposals

Advanced

Advanced Settings

☐ Enable Keep Alive

☐ Suppress automatic Access Rules creation for VPN Policy

☐ Require authentication of VPN clients by XAUTH

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

☐ Permit Acceleration

☐ Apply NAT Policies

☐ Allow SonicPointN Layer 3 Management

☒ Enable Phase2 Dead Peer Detection

Dead Peer Detection Interval(seconds):

180

Failure Trigger Level (missed heartbeats):

3

Management via this SA:

☐ HTTP ☐ HTTPS ☐ SSH ☐ SNMP

User login via this SA:

☐ HTTP ☐ HTTPS

Default LAN Gateway (optional):

0.0.0.0

VPN Policy bound to:

Zone WAN

Ready

OK

Cancel

Help

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

Outbound Interface:

Comment:

☒ Enable NAT Policy

Outbound Interface:

Comment:

☒ Enable NAT Policy

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:

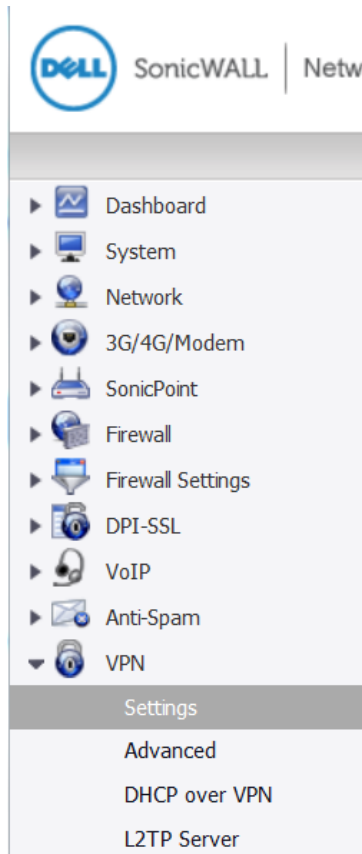
```
C:\Users\Administrator>ping 10.77.7.133 -t

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.

Kiosk VPN	65.217.255.43		10.77.7.133 - 10.77.7.133	ESP: AES-256/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	 
-----------	---------------	---	---------------------------	------------------------------	-------------------------------------	---

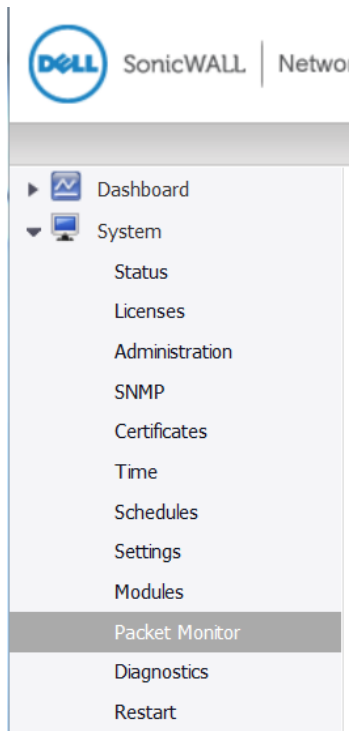
Hint: You may have to **uncheck and check the 'enable' box** pictured above to connect the first time.

Part 2

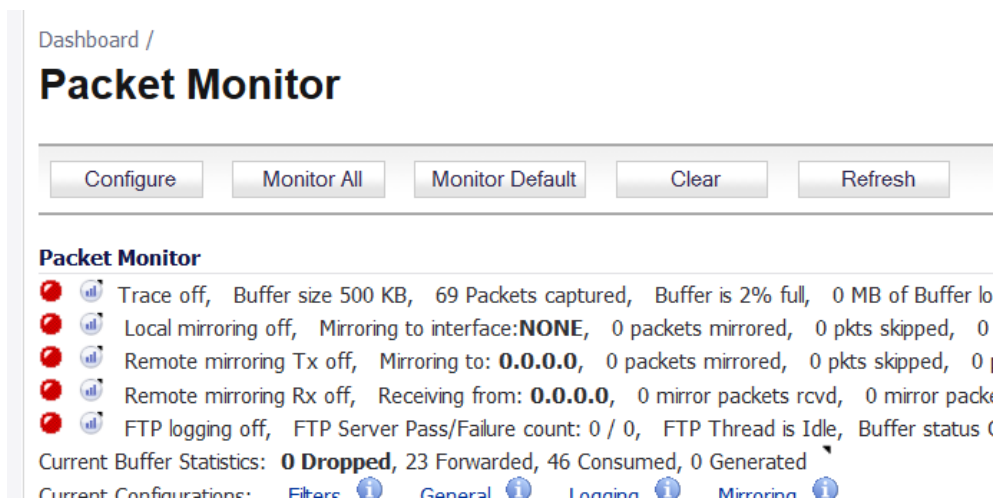
Setting up Packet Monitor to help troubleshoot connection problems

Basic setup


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



2) Click **Configure**



3a) Packet Monitor, Settings tab

 SonicWALL | Network Security Appliance

Settings Monitor Filter Display Filter Logging Advanced Monitor Filter Mirror

General Settings

Number Of Bytes To Capture (per packet):

☐ Wrap Capture Buffer Once Full.

Exclude Filter


☐ Exclude encrypted GMS traffic.

Exclude Management Traffic: ☒ HTTP/HTTPS ☐ SNMP ☐ SSH

Exclude Syslog Traffic to: ☐ Syslog Servers ☐ GMS Server

Exclude Internal Traffic for: ☒ HA ☒ SonicPoint

3b) Packet Monitor, Monitor Filter tab

 SonicWALL | Network Security Appliance

Settings Monitor Filter Display Filter Logging Advanced Monitor Filter Mirror

Monitor Filter (Used for both mirroring and packet capture)

☐ Enable filter based on the firewall/app rule

Interface Name(s):

Ether Type(s):

IP Type(s):

Source IP Address(es):

Source Port(s):

Destination IP Address(es):


Destination Port(s):

☒ Enable Bidirectional Address and Port Matching

Leave all checkboxes below unchecked for normal operation. Unchecked means capture all type of packets.

☐ Forwarded packets only ☐ Consumed packets only ☐ Dropped packets only

3c) Packet Monitor, Display Filter tab



Settings Monitor Filter **Display Filter** Logging Advanced Monitor Filter Mirror

Show (Display) Filter (Used for UI display only)

Interface Name(s):

Ether Type(s):

IP Type(s):

Source IP Address(es):

Source Port(s):


Destination IP Address(es):

Destination Port(s):

☒ Enable Bidirectional Address and Port Matching

☒ Forwarded ☒ Generated ☒ Consumed ☒ Dropped

3d) Packet Monitor, Advanced Monitor Filter tab



Settings Monitor Filter Display Filter Logging **Advanced Monitor Filter** Mirror

Advanced Filter

☒ Monitor Firewall Generated Packets. (This will bypass interface filter)

☒ Monitor Intermediate Packets.

- ☒ Monitor intermediate multicast traffic.
- ☒ Monitor intermediate IP helper traffic.
- ☒ Monitor intermediate reassembled traffic.
- ☒ Monitor intermediate fragmented traffic.
- ☒ Monitor intermediate remote mirrored traffic.
- ☐ Monitor intermediate IPsec traffic.
- ☐ Monitor intermediate SSL decrypted traffic.
- ☐ Monitor intermediate decrypted LDAP over TLS packets.
- ☐ Monitor intermediate decrypted Single Sign On agent messages.

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

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

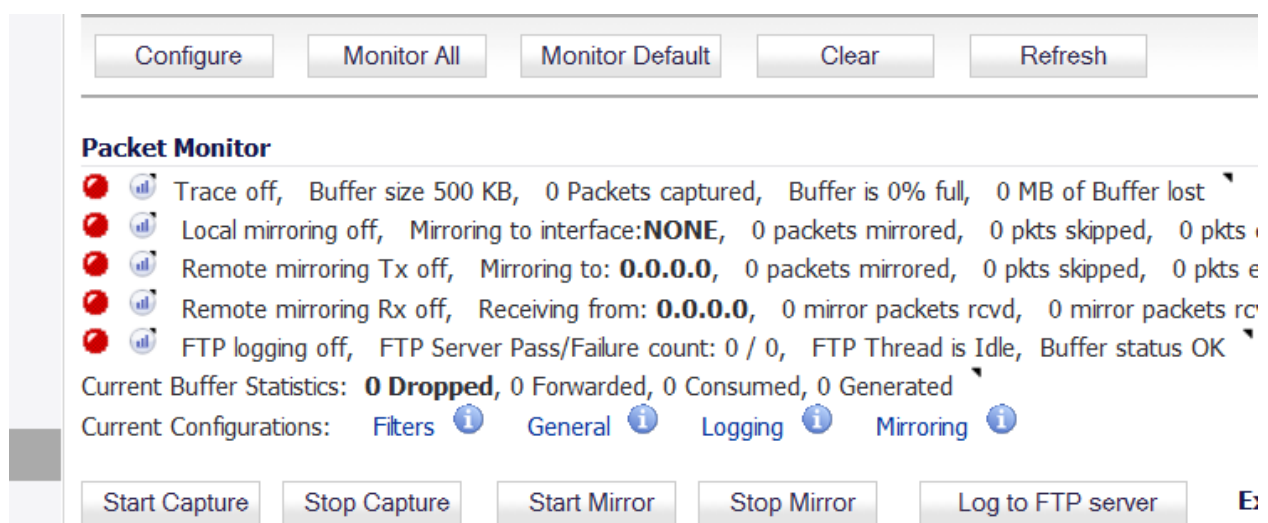
```
C:\Users\Administrator>ping 10.77.7.133 -t

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 (ICMP) every 10 minutes over the IPsec VPN from your kiosk or barcode computer to ensure the tunnel remains open and active all day

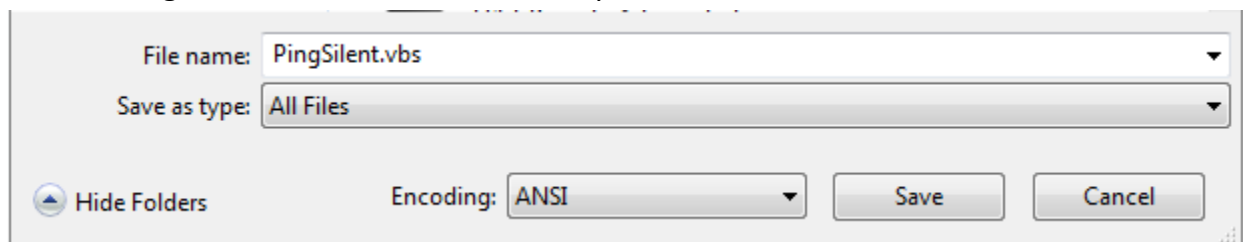
1) Log into your kiosk / barcode computer configured in step 1 of this document. Two files need to be created. Choose a location such as the local administrator desktop, and note the path, such as,

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

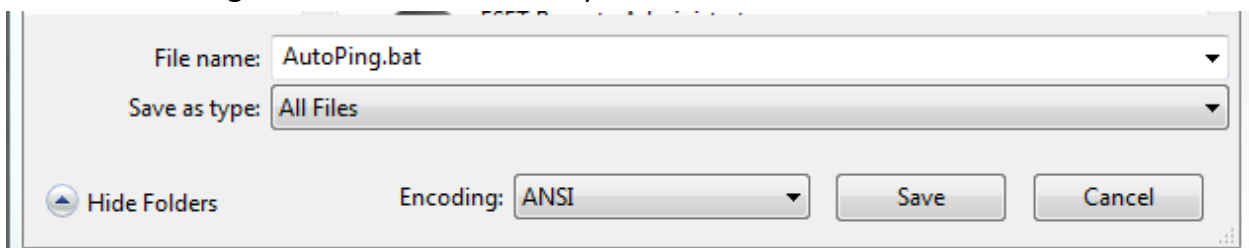


Be sure to change 'Save as type' from Text Document (*.txt) to **All Files**.

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.

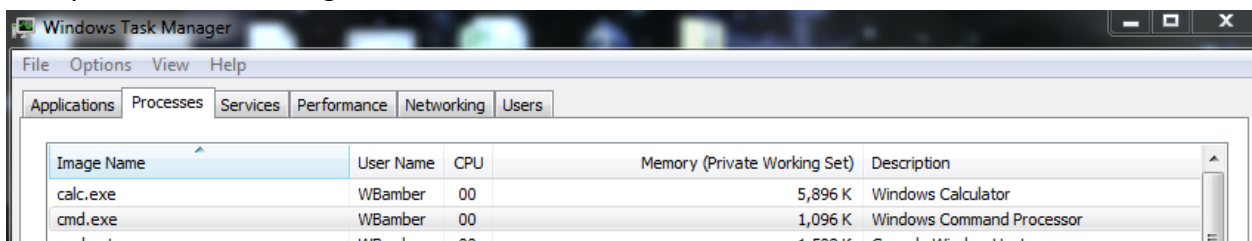
PingSilent.vbs opens **AutoPing.bat** and causes **cmd.exe** to run **silently**. Nothing pops up or is indicated on the taskbar.

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:

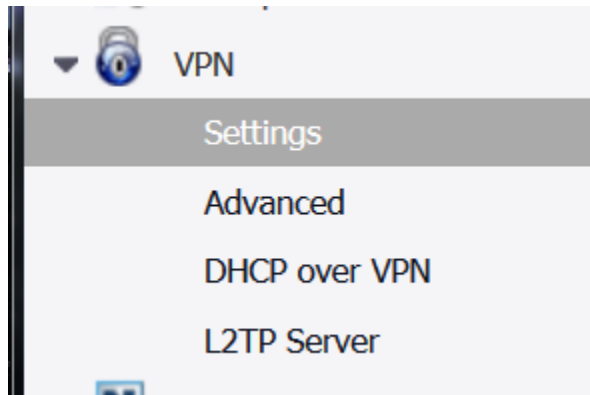


5b) Verify tunnel can be triggered open, and traffic is flowing

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.

A screenshot of the 'VPN Policies' table in the SonicWALL interface. The table has columns for #, Name, Gateway, Destinations, Crypto Suite, Enable, and Configure. The first row shows a policy named 'Kiosk VPN' with a green status icon in the 'Enable' column.

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
5	Kiosk VPN	65.217.255.43	10.77.7.133 - 10.77.7.133	ESP: AES-256/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

(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

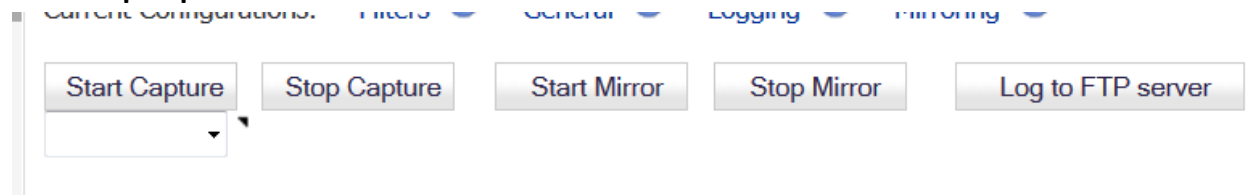
Verify the IPsec Tunnel is now open ("**green light**")

A screenshot of the 'VPN Policies' table, identical to the one above, but the status icon in the 'Enable' column for 'Kiosk VPN' is now a solid green circle, indicating the tunnel is open.

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
5	Kiosk VPN	65.217.255.43	10.77.7.133 - 10.77.7.133	ESP: AES-256/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

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

Click **Stop Capture**.



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

Captured Packets Items: 1 10/21 (Of 21) 14 4 1

#	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