# PNF FW HANDOVER

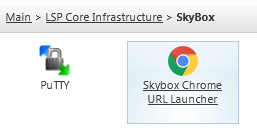
* **Day 0 –** Requirements issued into the Master Sheet – [(Master sheet link)](https://collab.rbsres01.net/teams/ecp-in-dcnrr-3k6tgvhj/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2fteams%2fecp%2din%2ddcnrr%2d3k6tgvhj%2fShared%20Documents%2fFirewall%20Rules%20and%20Contracts%20%28MG%20and%20MM%20DCs%29&FolderCTID=0x0120002362542DA2E71E4486447F1BD03E007B) by 3rd party Vendors.
* **Day 1 – Analysis begins** 
  + Validating requirements with the owner of the reqs and ask them questions. Is there anything missing from the Master Sheet – port details, directionality, general clarification etc.
  + Assigning appropriate firewall and DC details.
    - MM PNF IP’s = 10.118.X.X range
    - MG PNF IP’s = 10.116.X.X range
    - 10.135.X.X = MM & MG
    - We can also traceroute IP’s to find which firewall they are behind.
    - We can utilise the “networks” tab within the master sheet to appropriately assign PNF IP’s.
  + Assignment of appropriate hostname to IP’s and the grouping of hosts where necessary.
    - Simply use the “**nslookup** **x.x.x.x**” command within CMD prompt to find the respective hostname within the DNS record. If missing reach out to req requester. If the requestor is unable to provide the hostnames in time then use a temporary name such as “HOST-X.X.X.X”.
  + Confirm that the requirements are necessary, there maybe an existing rule(s) within the firewalls.
    - For LSP Zone 6 FW changes there exists a blanket rule between LSP Zone 6 and PNF within the policy under policy ID’s: **1003108 & 1003109**.
    - We can also use SB to confirm whether the rule is required by inputting and saving the rule there before observing the result within “required?” column:

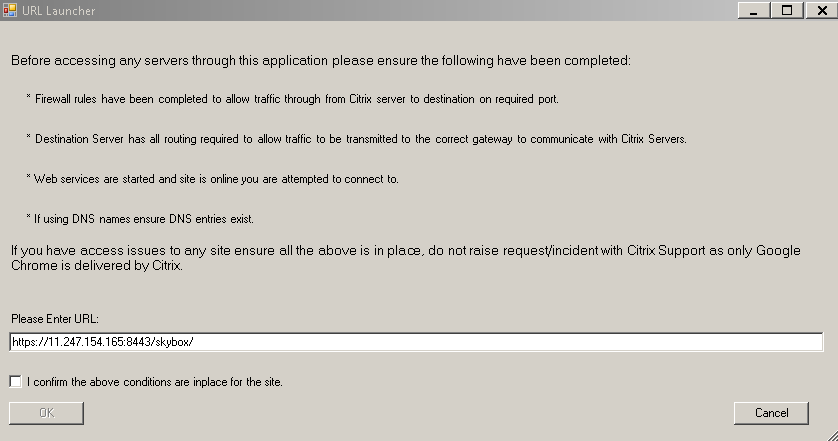


* + We conduct the analysis on a local copy of the master sheet. Need to upload to the ECP shared drive so that the analysis is readable and accessible.
* **Day 3 – Analysis Ends**

SB Ticket Phase

We can access SB through the below URL launcher within CAG:





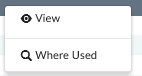
Use this link (**https://11.247.154.165:8443/skybox/**) as seen within the above launcher to launch SB.

* **Day 3 – Populate and promote the SB ticket and get into TLV as soon as possible**
  + Main **contacts for TLV**: ([Ravindra-Kumar.Sinha@rbs.co.uk](mailto:Ravindra-Kumar.Sinha@rbs.co.uk), [Chandra.Prakash@rbs.co.uk](mailto:Chandra.Prakash@rbs.co.uk)).
* **Day 5 – Finalise the SB ticket and promote into the PCSA stage**
  + Main **contacts for PCSA**: (~ Perimeter Security – Change Advisory [FM-036871@rbos.co.uk](mailto:FM-036871@rbos.co.uk), [Piotr.Cichon@rbs.com](mailto:Piotr.Cichon@rbs.com), [Daniel.Parnak@rbs.com](mailto:Daniel.Parnak@rbs.com), [Michal.Warzynski@rbs.com](mailto:Michal.Warzynski@rbs.com)), [Pawel.Pachnia@rbs.com](mailto:Pawel.Pachnia@rbs.com). (**This team is mainly based in Poland and are often offline after 15:00 UK).** 
    - Reach out to the above resources to find out who your SB ticket has been assigned to within their team. (This is the individual who will be reviewing your ticket).
  + PCSA team will take a day to reply back to you with any questions if necessary.
  + Email Chain Example
* **Day 6 – Answer the questions from the SB team and get promoted to ROA**
  + If we need to provide port justification for the requirements that have been provided, there are two options:

**1.** If the port is new; revert back to the requester of that requirement within the mail thread.

**2.** If the port is existing; find the SB ticket it was previously requested under,

* + - To find the SB tickets go to the appropriate ADOM within the FortiManager for the rule in question. **->** object configurations **->** services. Search for the port and right click on it and select where used.



This will display the rules that contain this port. Simply view each rule and record the SB ID’s within comment left in the description section. For example a comment follows the following syntax (SB ID in bold):

TCRxxxxxxx:SBID-**1234**:01-01-2018:Shillsa.

* + When the ticket is promoted to ROA, we need to provide the summary of the requirements to the rule owner (For PNF this is Gareth Morrison). Reach out to the req requestors for this and share it.
    - After the summary is sent to him we have a lead time of 24 hours with Gareth for his approval.
  + Equally, make sure that we speak to the SB MS team ([**Gemma.Coghlan@rbs.co.uk**](mailto:Gemma.Coghlan@rbs.co.uk)and [**Chris.A.Peach@rbs.co.uk**](mailto:Chris.A.Peach@rbs.co.uk)) to send out the email requesting the rule owner’s approval.
  + Example of change summary email 
  + Example of approval email. 
* **Day 7 – the ticket is promoted into Implementation State, the TCR can be put into Ready for Auth.**

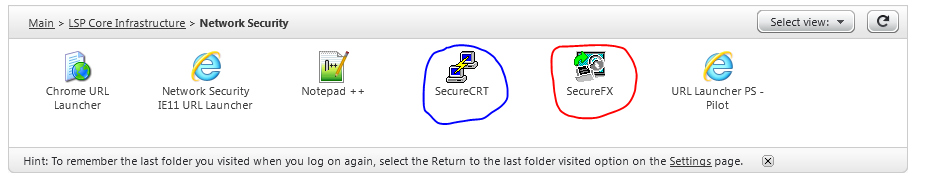
Implementation

* For the pre-change checks at 16:00 on the day of the implementation, we need to submit the elevation request a day or at least 5 hours prior to the change to **“~ Network Services Security Elevation** [**FM-036018@rbos.co.uk**](mailto:FM-036018@rbos.co.uk)**”** (for both the ADOMs and the VDOMs):
  + Use the same table format and subject as seen within the elevation email example: 
* Chase the team for elevation 10-20 mins ahead of your change.

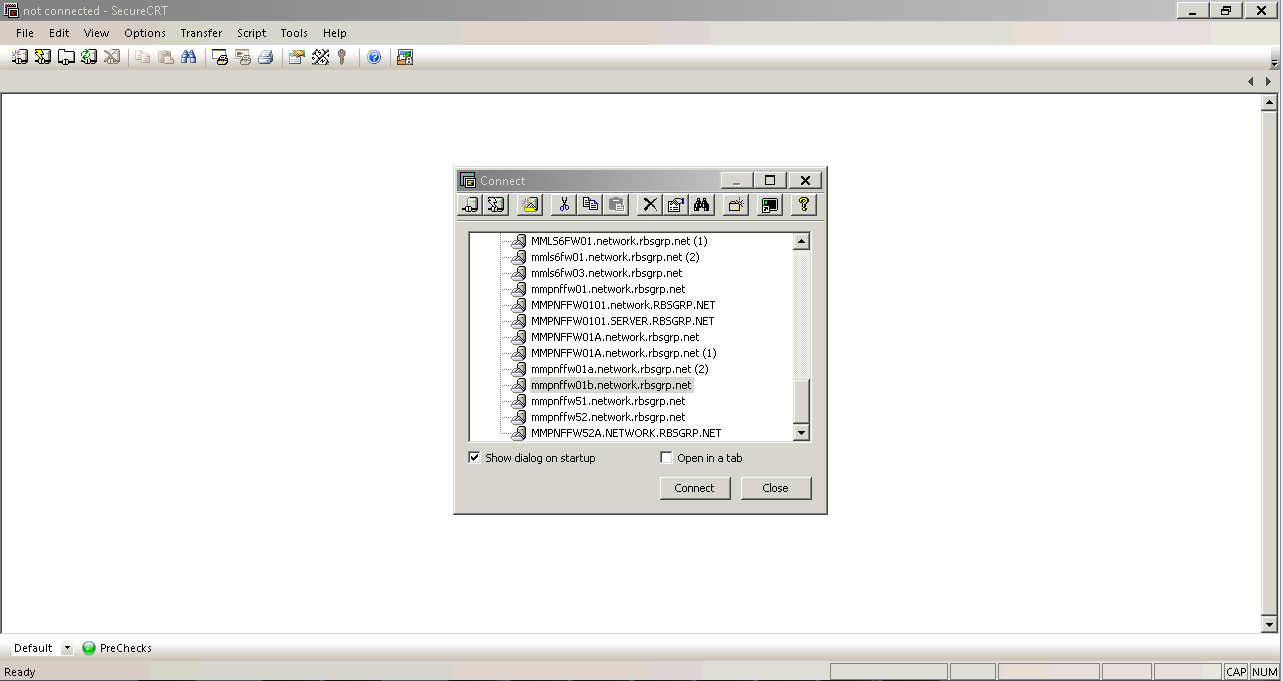
Pre/Post Change checks

Take pre/post-checks from the CLI of MGPNFFW01A.NETWORK.RBSGRP.NET & MMPNFFW01B.NETWORK.RBSGRP.NET.

* Within CAG open secure CRT as seen below.



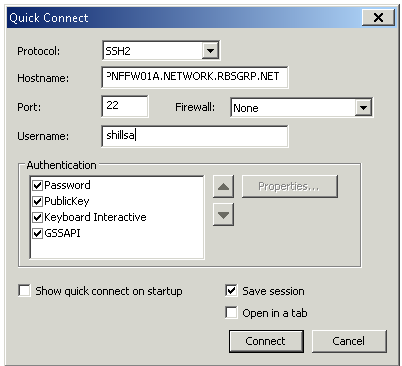
* It should look like this once open:



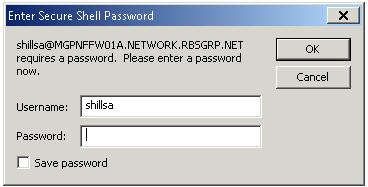
* Select Quick connect:



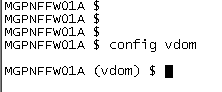
* Insert the devices hostname and your RACF as seen below and select connect:



* Enter your password and select ok:



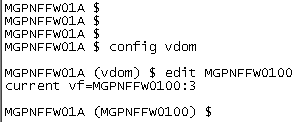
* Once logged in select file -> Log session.
* Find the folder under your RACF within the “CTXDATA” drive and save your session there. For example you can save it as “MGPNFFW01A post config backup.log”.
* Insert into the cli “config vdom”:



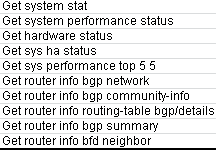
* Press tab until the word “edit” appears:



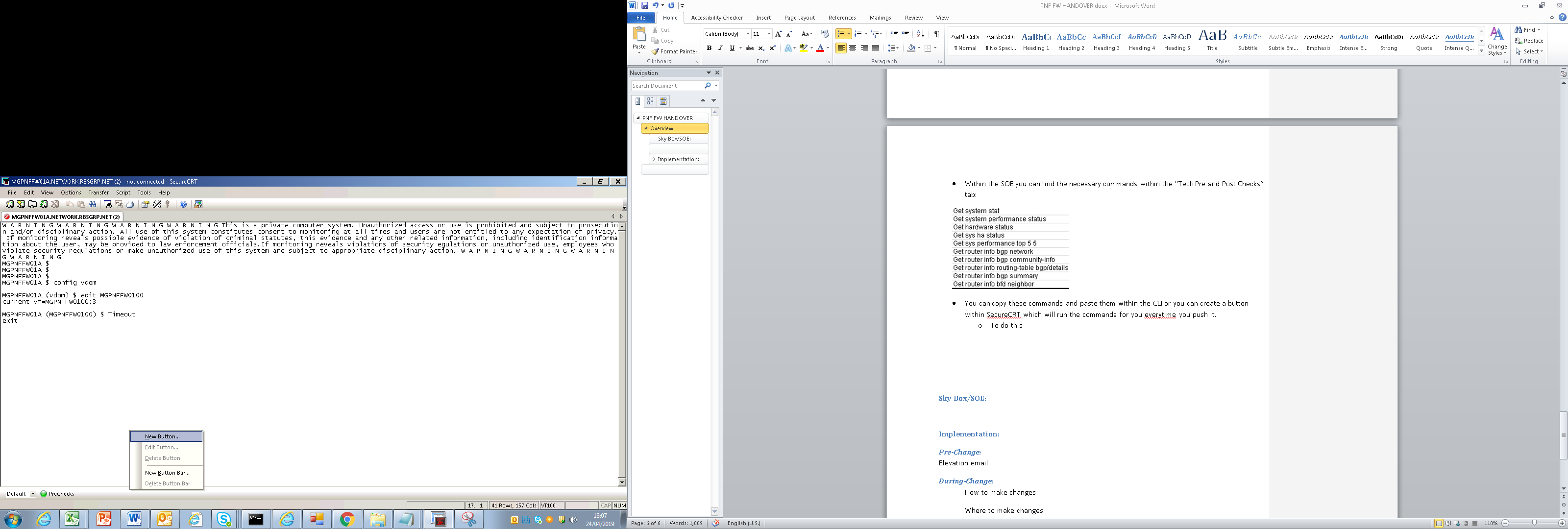
* Press space and then tab again until you see either “MGPNFFW0100” (MG DMZ VDOM) or MGPNFFW0101 (MG MGMT VDOM) and press enter. **(Please note that these steps are required for both MGMT and DMZ VDOMS).**



* Within the SOE you can find the necessary commands within the “Tech Pre and Post Checks” tab:



* You can copy these commands and paste them within the CLI or you can create a button within SecureCRT which will run the commands for you every time you push it.
  + To do this right click the bottom bar and “select create new button”:



* + Paste the commands in there in the following format (with \n at the end of each line):
    - get system stat \n

get system performance status \n

get hardware status \n

get sys ha status \n

get sys performance top 5 5 \n

get router info bgp network \n

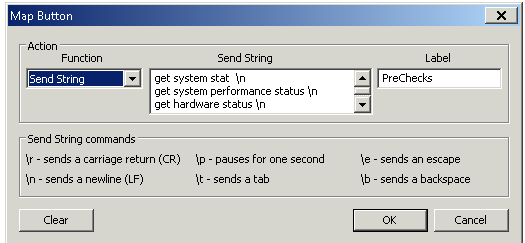
get router info bgp community-info \n

get router info routing-table bgp \n

get router info bgp summary \n

get router info bfd neighbor \n

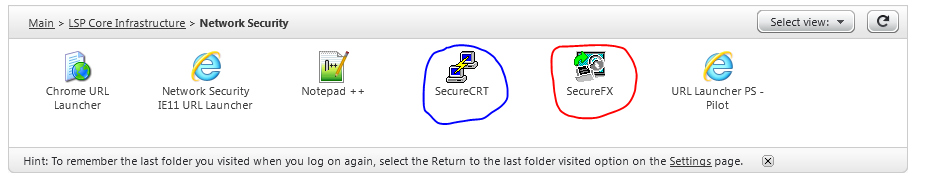
* + Label your button and then select ok:



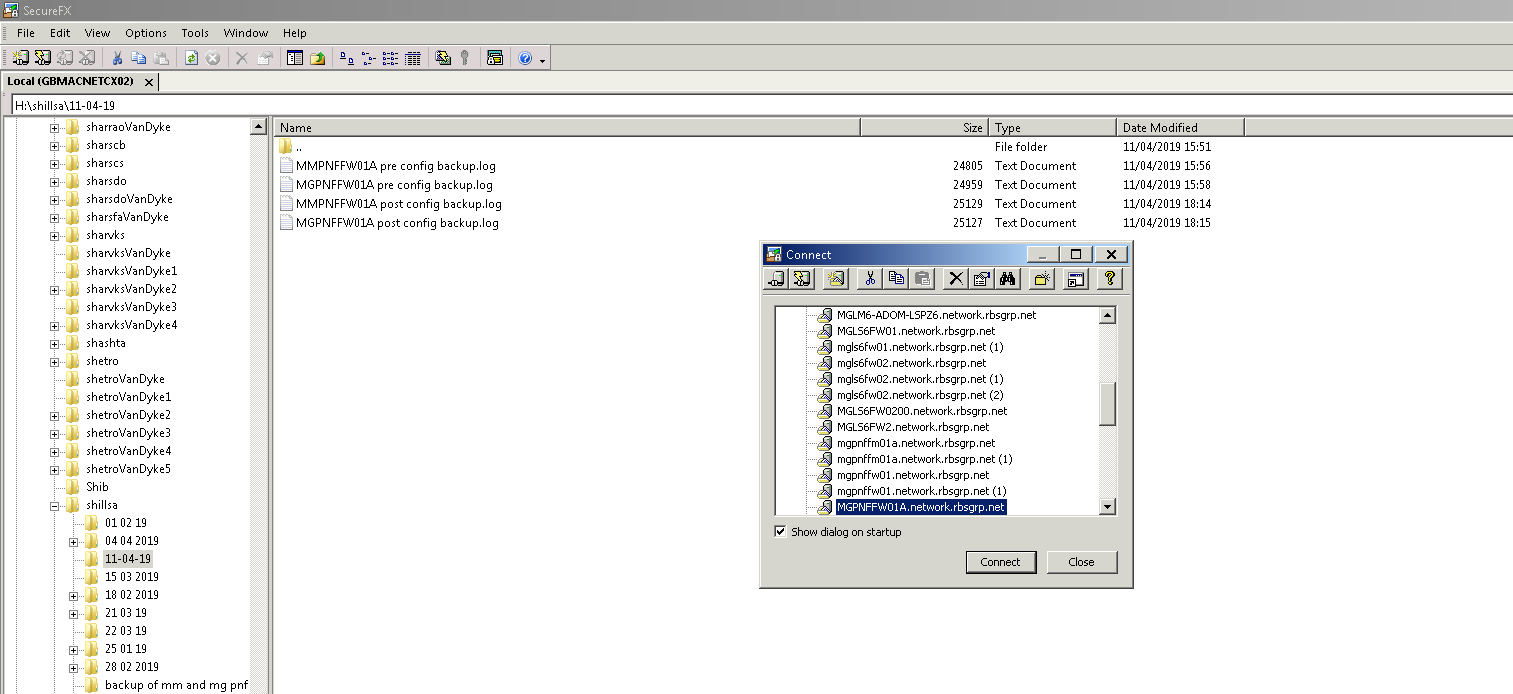
* + Once this button has been created you can press it to take pre-checks for both MGPNFFW01A.NETWORK.RBSGRP.NET & MMPNFFW01B.NETWORK.RBSGRP.NET and any other checks you may need to do in the future.

Repeat the above process for post change checks.

* Once you’re elevated prep the change.
* Once the change has been prepped, share the policy with peer reviewer.
* The peer reviewer needs to analyze the policy against the SB ticket.
* Once the peer reviewer gives the go ahead, then you’re okay to push the change at 18:00.
* Once the change has been pushed take post-checks as explained earlier.
* Update the wider team and share the pre and post logs:
  + To get the logs you saved, within CAG select SecureFX



* SecureFX should look like the below:



* Close the “Connect” window and use the left window to find your files.
* Open your files and copy and paste the contents into a new notepad and save it.