VPN between DataCentre and Paktronix including Roaming

MGM, JD, NSA, CISA, CISSP

This is a scenario of a VPN structure between Paktronix core network, the Remote DataCentre network, and Paktronix roaming engineers. The scenario covers both StrongSwan IPSec VPN connections and WireGuard connections including a WireGuard bridge connection between the DC primary and DC secured networks. The setup for allowing roaming access to the Paktronix network is also illustrated.

PakVPN – WG Roaming –> PakFW

This setup uses an Ostiary called from the roaming machine to insert/enable and deinsert/disable the WireGuard structure with a specific IPtables hole for the WG VPN

Ostiary Port: 12345 / Always enabled in FW – FILES: RemoSTART.sh / RemoSTOP.sh

When Ostiary is correctly triggered it inserts IPtables rules to allow REMO UDP WG port <-> PakFW UDP WG port. It then inserts, starts and enables the WG instance for REMO and finally inserts a NAT command to allow REMO to access the internal networks. On close it reverses these operations.

WireGuard UDP Port: PakFW = 54321 / REMO 43210 (Security discussion)

PakFW : 7.6.5.4:54321 – **JumpServer** - FILES: PakCorpFW.pakvpn (same as SS/WG)
VPN IP : 10.7.7.254/32, 172.18.1.0/24, 192.168.2.0/24, 192.168.23.0/24

PakREMO: N/A:43210 – NO Known IP addr!! - FILES: PakREMO.pakvpn
VPN IP : 172.18.1.1/32

PakVPN – SS & WG – Pak<->DC

WireGuard UDP Ports: Pak = 7250 : DCFW = 333xx

PakFW : 7.6.5.4:7250 – **JumpServer** –
FILES: PakCorpFW.pakvpn / wgudp-NAT.wgfw
VPN IP : 172.16.2.0/24, 192.168.2.0/24, 192.168.23.0/24

DCFW01: 6.7.8.9:33309
VPN IP : 172.16.2.31/32, 10.7.7.31/32, 10.1.2.0/24

DCFW02: 5.6.7.8:33308 – **DC Internal JumpServer** –
FILES: DCFW02-PakCorpFW.WGstart / DCFW02-Conf.pakvpn / dc2pak-wginterface-FWD.wgfw
VPN IP : 172.16.2.32/32, 10.7.7.32/32, 10.2.1.0/24
VPN DC INT: 10.7.7.111/32, 10.7.7.112/32, 192.168.33.0/24

StrongSwan IPSec:

PakFW : 7.6.5.4
FILES: PakCorpFW-StrongSwan.sh / PakCorpFW-SS.ipsec.conf / PakCorpFW-SS.swanctl.conf
VPN IP : 172.17.2.0/24, 192.168.2.0/24, 192.168.23.0/24

DCFW01: 6.7.8.9
VPN IP : 172.17.2.31/32, 10.1.1.0/24

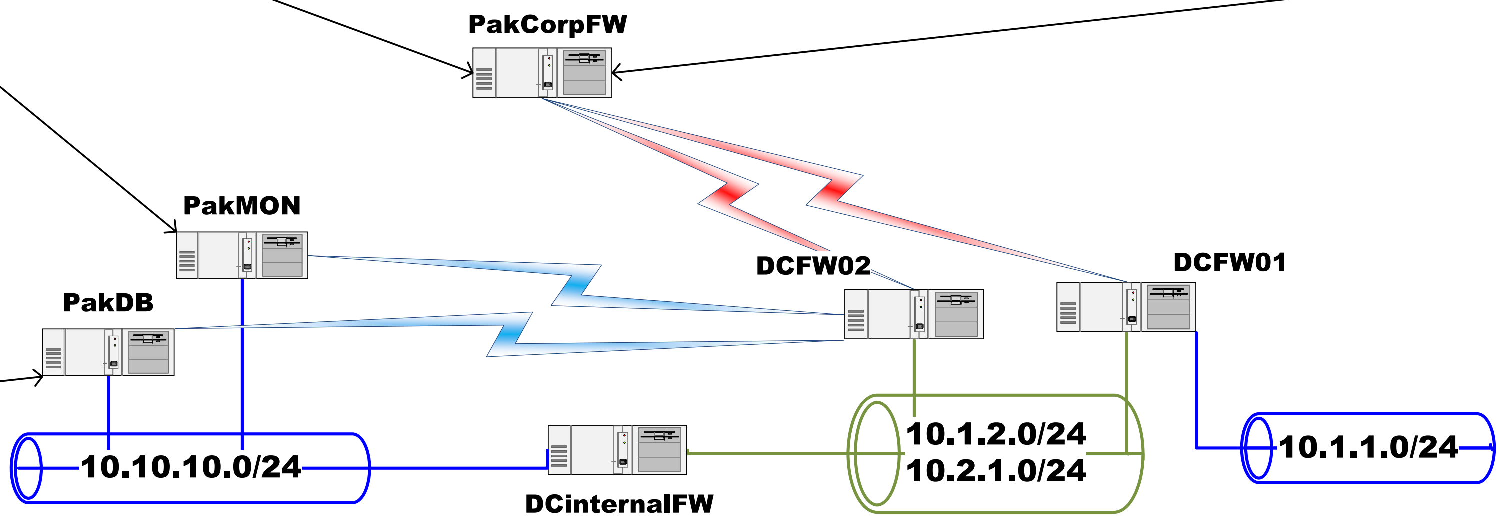
PakVPN – WG – DC Internal

UDP Port: 33316

PakDB: “111 machine”
PakVPN PR = pakwg0 = 10.7.7.111/32
WG = dcintdb = 192.168.33.111/32

PakMON: “112 machine”
PakVPN PR = pakwg0 = 10.7.7.112/32
WG = dcintmon = 192.168.33.112/32

DCFW02: “2/32 machine” - **JumpServer**
NOTE that this uses 2 AND 32 (32 from PakWG)
PakVPN PR = pakwg0 = 10.7.7.32/32
WG = dcint = 192.168.33.2/32



LEGEND

TRUSTED (Internal)
Eh-Whatever (DMZ)
UNTRUSTED (External)

Created 30-Nov-2020
Modified 28-Feb-2021

Diagram Courtesy of Paktronix Systems LLC, 1602 North 59th Street, Omaha NE 68104-4832, All Rights Reserved