**Divestment Checklist**

**\*Note:** The below devices are assumed to have the standard base configurations applied to them.

**Internet Border Router**

Configure VRF43 for internet traffic

Configure standard INBOUND and OUTBOUND firewall filters which include anti-spoofing and high-port blocks as well as other standard terms

**NORTH Firewall**

Create inbound internet rules for CorpVPN North access

Create inbound internet rules for TPRAS VPN North access

Create inbound internet rules for S2S VPN North access

Create inbound internet rules for F5 VIPs North access

Create VRF58 for North DMZ traffic

Create IPS policy with Variable Set via FMC for FTD devices

Create Security Intelligence (i.e. blacklist sites) policy assigned to screening interface via FMC for FTD devices

**SOUTH Firewall**

Create inbound DMZ rules to internal corporate network for CorpVPN South access

Create inbound DMZ rules to internal corporate network for TPRAS VPN South access

Create inbound DMZ rules to internal corporate network for S2S VPN South access

Create inbound DMZ rules to internal corporate network for F5 services South access

Create VRF59 for South DMZ traffic

Create IPS Policy with Variable Set via FMC for FTD devices

**EXTRANET**

Configure interface for point-to-point external customer circuit on WANRTX router

Configure VRF for each customer and routing between WANRTX router to extranet firewall. (VRF117 was used for IBM Syncrude and MP-BGP was used for the routing between the WANRTX router and firewall.)

If using the IBM connection in Dallas as the extranet connection, reserve and update [Master - Divestment NAT Allocations](https://ishareteam1.na.xom.com/sites/FIGATEWAY/IH/Connectivity%20Documentation/Extranet%20Standards/Master%20-%20Divestment%20NAT%20Allocations.xlsx) spreadsheet for inbound and outbound NAT subnets. If using RFC1918 address space, check with new company that there is no IP overlap.

Configure firewall rules and NATs using standards defined in [Extranet Standard for Divestments](https://ishareteam1.na.xom.com/sites/FIGATEWAY/IH/Connectivity%20Documentation/Extranet%20Standards/Extranet%20Standard%20for%20Divestments.docx) document which includes naming conventions for objects

Create IPS Policy with Variable Set via FMC for FTD devices

**CORPVPN**

Allocate and reserve CorpVPN pool in the new IPAM/DNS (ex: Infoblox) server. (The new servers must be ready before reserving the pool. Also, check with new company that there is no RFC1918 overlap.)

Submit request to DNS team to reserve DHCP scopes for CorpVPN pool on DHCP servers.

Submit request to AD/PKI team to update the “WCL-Comp-WDF” GPO used by SentinelOne to allow outbound access to the outside IP of the new CorpVPN gateway. (This will need to be applied to both XOM and new company AD servers.)

Submit request to AD/PKI team to replicate “**XSnetsecaccp**” (acceptance) service account in new AD servers which is used for AD LDAP queries for machine certificate authentication. **DO NOT use prod corp vpn service account "XSnetsec" for any divestment activities.**

Generate CSR on new CorpVPN gateway and submit to AD/PKI team to create temporary SSL certificate using XOM CA

Generate another CSR on new CorpVPN gateway and submit to AD/PKI team to create final SSL certificate after new divestment CA is built. (While the trustpoint for this SSL certificate can be created, it should not be applied to the outside interface to be used until CiC.)

Create new XML profile for user workstations that will be divested

Create new VPN mgmt. tunnel profile for user workstations that will be divested. This file must be called VpnMgmtTunProfile.xml in order for the VPN mgmt. tunnel to work. (Information regarding the Cisco VPN Mgmt Tunnel feature can be found on this document: [VPN-MgmtTunnel-InternalUse](https://ishareteam1.na.xom.com/sites/FIGATEWAY/Transport/Connectivity/VPN-MgmtTunnel-InternalUse.docx))

Submit request to DNS team to provide DHCP for VPN pool and append specific DNS suffix (e.g. sa.xom.com) to the IPs assigned out. (This is needed in order for the user workstations to register themselves in DNS so that the EMG migration team can find the user workstations remotely over VPN using the machine names to run their migration scripts.)

Configure VPN gateway to use separate DHCP servers to handle DHCP of the VPN pool

Configure VPN gateway to use VPN mgmt. tunnel functionality

**TPRAS VPN**

Generate new CSR on TPRAS gateway and provide to new company in order for them to create an SSL certificate using their own external vendor (e.g. DigiCert, Entrust, GoDaddy, etc.)

Allocate and reserve TPRAS VPN pool in new IPAM/DNS (ex: Infoblox) server. (Check with new company that there is no RFC1918 overlap.)

Configure clientless (i.e. TPRAS access using a browser) access for vAppConnect

Configure rules for clientless access on the DMZ South firewall and not the TPRAS VPN gateway itself since it acts a reverse-proxy for the connection. Source IP will be the “inside” interface IP that will show up on the DMZ South firewall.

Configure client-based (i.e. TPRAS access using Cisco AnyConnect client) access

Configure rules for client-based access on the TPRAS gateway itself as it acts as a proxy and firewall combo

Create new TPRAS XML profile for third-party users

Configure 2FA with external authentication as it is required for third-party users to use the TPRAS service

**S2S VPN**

Exchange relevant S2S tunnel parameters with third-party for Phase1/Phase2 negotiations (e.g. peer IP, encryption parameters, etc.)

Configure S2S tunnel using the tunnel parameters obtained from the third-party

Create firewall access rules for the service that is using the S2S tunnel

If S2S connectivity is with IBM, duplicate firewall rules and NATs exactly the same as in Dallas. (Routing cutover info here.) follow instructions regarding allocating NAT subnets in [Master - Divestment NAT Allocations](https://ishareteam1.na.xom.com/sites/FIGATEWAY/IH/Connectivity%20Documentation/Extranet%20Standards/Master%20-%20Divestment%20NAT%20Allocations.xlsx) spreadsheet and access/NAT rule creation standards including naming conventions from Extranet Standard for Divestments

**F5 Services**

Purchase virtual F5 BIG-IPs if F5 services are needed. (Purchase one for internal F5 services and a separate one for DMZ/internet-facing services.)

Virtual BIG-IP should be created with the following VMWare requirements:

LTM only : 4 CPU cores, 8 GB memory, 40 GB storage

LTM + APM : 8 CPU cores, 16 GB memory, 80 GB storage

Configure F5 VIP according to requirements provided by the business

If F5 VIP requires an SSL certificate, generate new CSRs on F5 BIG-IP guest and provide to new company in order for them to create SSL certificates using their own external vendor (e.g. DigiCert, GoDaddy, etc.)

Trunk the virtual F5 DMZ VLAN subnets from the VMWare hosts using Layer-2 trunking through to the DMZ core

**Cisco FMC**

Purchase virtual FMC with 10 node license if FTDs and/or SFR modules are being used. (Buy larger node license if there are more than 10 FTDs.)

Virtual FMC should be created with the following VMWare requirements: 4 CPU cores, 32 GB memory, 250 GB storage

FMC licensing is handled through the XOM satellite server. (Aditya Sagar / Jorge E Reyes can add the license to the satellite server and generate the token needed to register the FMC.)

For FMC licensing at CiC, the FMC will need to be re-configured to connect directly to the Cisco cloud instead of using the satellite server. (Aditya / Jorge can assist with generating the necessary token for a “default” account for Cisco cloud. This will then allow the new company to transfer the licenses to their own smart account.)

**Miscellaneous Notes**

Use BGP as default standard routing protocol wherever possible. Static routes can be used if necessary.

For initial build, XOM standards and configuration can be used. However, at CiC, any XOM related information should be removed or updated to the new company devices.

If there are services in which users are assigned public IP addresses (either through a VPN pool or DHCP scope for example), then a request will need to be submitted to the Outbound Internet team to update the iBoss PAC file/policy to include the public subnet.

**Cleanup (after CiC):**

Submit individual POR requests to decommission each third-party NECTs (for S2S and TPRAS)

Submit POR request to delete customer divestment firewall rules, NATs, and objects from NECT1977 (for Dallas IBM connectivity)

Submit POR request to update WANRTI INBOUND/OUTBOUND filter rules if public address space is moving to new company

Submit request to AD/PKI team to revoke any temporary SSL certificates generated by XOM CA for divestment purposes

Submit requests to delete any DNS entries for network devices that were involved with the divestment

Submit requests to deregister any ISE/TACACS allowed for network devices that were involved with the divestment

Submit request to remove CorpVPN outside interface IP from “WCL-Comp-WDF” GPO for SentinelOne from XOM AD servers