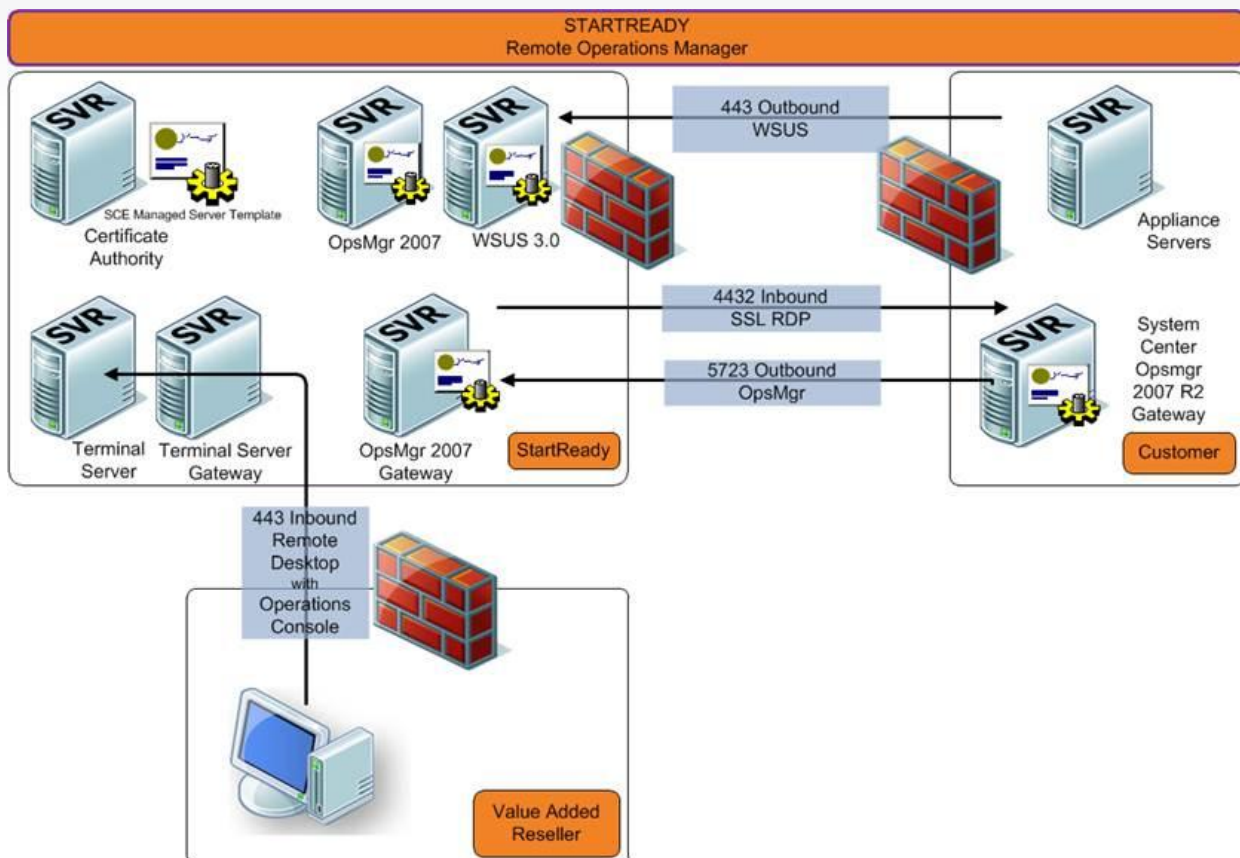


StartReady Appliances Appliances are implemented inclusive of a total maintenance solution. This means 24*7 monitoring, remote support, patch management and adhering to the agreed-upon SLA.

During the implementation of a StartReady Appliance, Microsoft management software is installed. This is System Center Essentials 2007 (SCE). SCE is used by StartReady for:

- Remote Access;
- Monitoring;
- Windows Updates.

The following architectural overview paints a picture of the software and communications.



Remote Access

For remote access, StartReady uses a secure SSL Remote Desktop session. Communication between StartReady's datacenter and the customer's appliance is done via port 4432. The communication is secured using an SSL certificate. We expect the customer to open port 4432 for communication from StartReady. This port can be specifically opened to only accept communication from startready.com or its IP address. Access for our partners is managed via our environment.

Monitoring

In order to meet our 24*7 SLA, proactive monitoring is part of every StartReady Appliance. This monitoring ensures that all Windows Events of the supplied Microsoft software are forwarded to the StartReady Monitoring environment. On the Appliance, SCE will be put in "Service Provider Mode" and will function as a pass-through hatch. The events pass through our Operations Manager Gateway inside System Center Operations Manager (SCOM). SCOM will use the Microsoft Management Packs for the analysis and, where necessary, report back to the StartReady Support desk. The required communication is done via port 5723 from the client side to the StartReady datacenter.

Microsoft Updates

StartReady takes full responsibility for keeping the Microsoft software up-to-date on the Appliance. This is done based on updates released by Microsoft through Windows Update. In case the software is self-installed or self-managed, the software will be pointed to the Microsoft's WSUS environment (or the client's) in order to download the latest updates. The software installed on a StartReady Appliance is pointed to the WSUS environment at StartReady. This allows StartReady to test the updates internally first. This is done both at StartReady, and at a group of select pilot customers. Once this is deemed a success, the updates are released to the Appliances. The WSUS environment on the Appliance will keep its catalog in sync with the StartReady WSUS environment. When updates are released, these will be downloaded on Microsoft's side. Reboots (when required) are done in the middle of the night. The required communication is done via 443 over the internet.

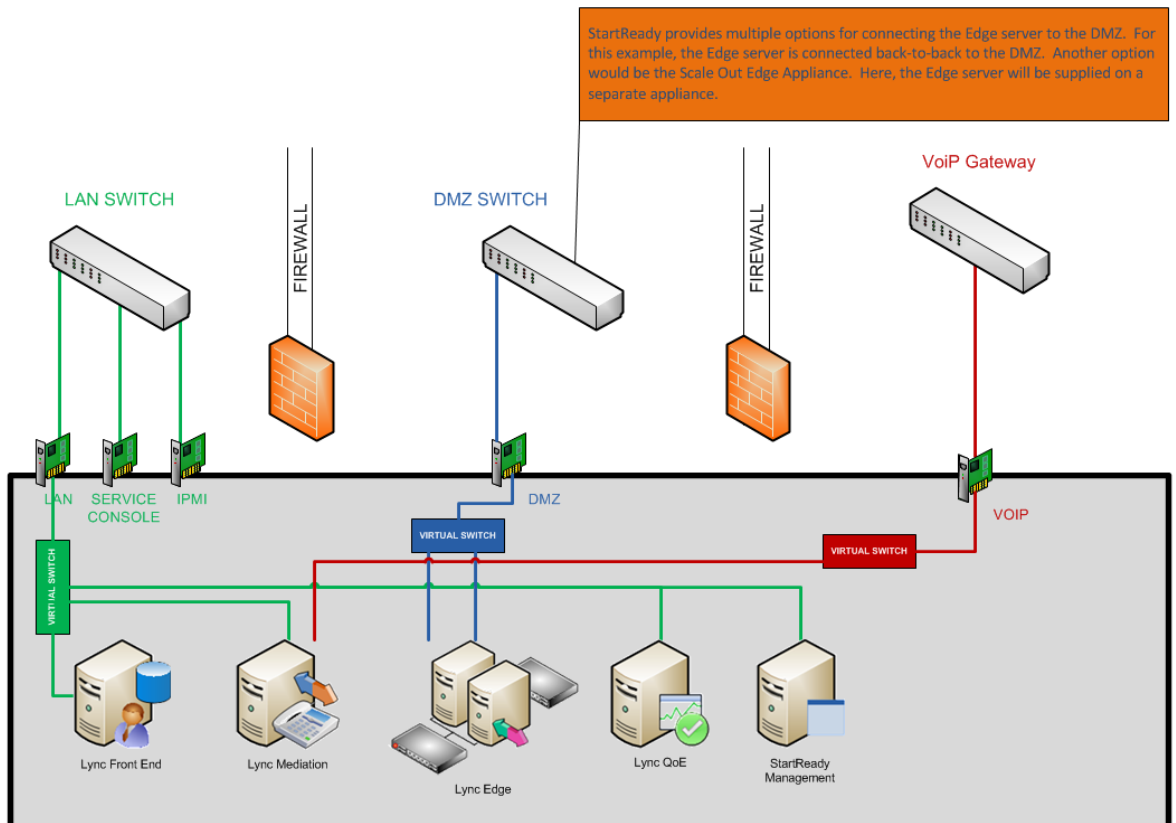
StartReady Appliance in the IT infrastructure.

The wiring diagram shows both the physical network connections as well as the virtual network connections. The physical connections are connected to these different networks:

1. LAN (Local Area Network)
2. Management LAN (this is optional for the service console and/or the IPMI interface)
3. DMZ (Demilitarized Zone)
4. Internet Switch (this can be in the DMZ, but in that case the firewall cannot apply NAT).¹

The virtual network connections are connected by means of the physical network connections to the virtual servers on the appliance.

Below is a wiring diagram of a Lync Appliance. In this example, we chose for an Appliance which is connected to a SIP trunk. If another form of telephony integration is chosen, the VOIP connection can be adjusted.



¹ The SIP protocol doesn't support NAT (Network Address Translation). When NAT is applied, the solution will not function properly.

There are a total of five physical network connections:

1. LAN-Local Area Network — This network connection connects all the virtual servers on the LAN infrastructure via the virtual switch.
2. Service Console— This host server of all the virtual machines connects to the physical appliance to the LAN.
3. IPMI- Intelligent Platform Management Interface — Connects the IPMI to the LAN. IPMI is used for any support should the physical server (using normal interfaces) no longer be accessible.
4. DMZ-Demilitarized zone — This network connects the “Lync Edge” to the DMZ via the virtual switch. The Lync Edge is a Lync server role that delivers communication to external internet connections.
5. VOIP — This network connection connects the “Lync Mediation” to the SIP trunk provider via the virtual switch. This connection needs to be transparent en cannot be connected to the appliance via NAT (Network Address Translation).