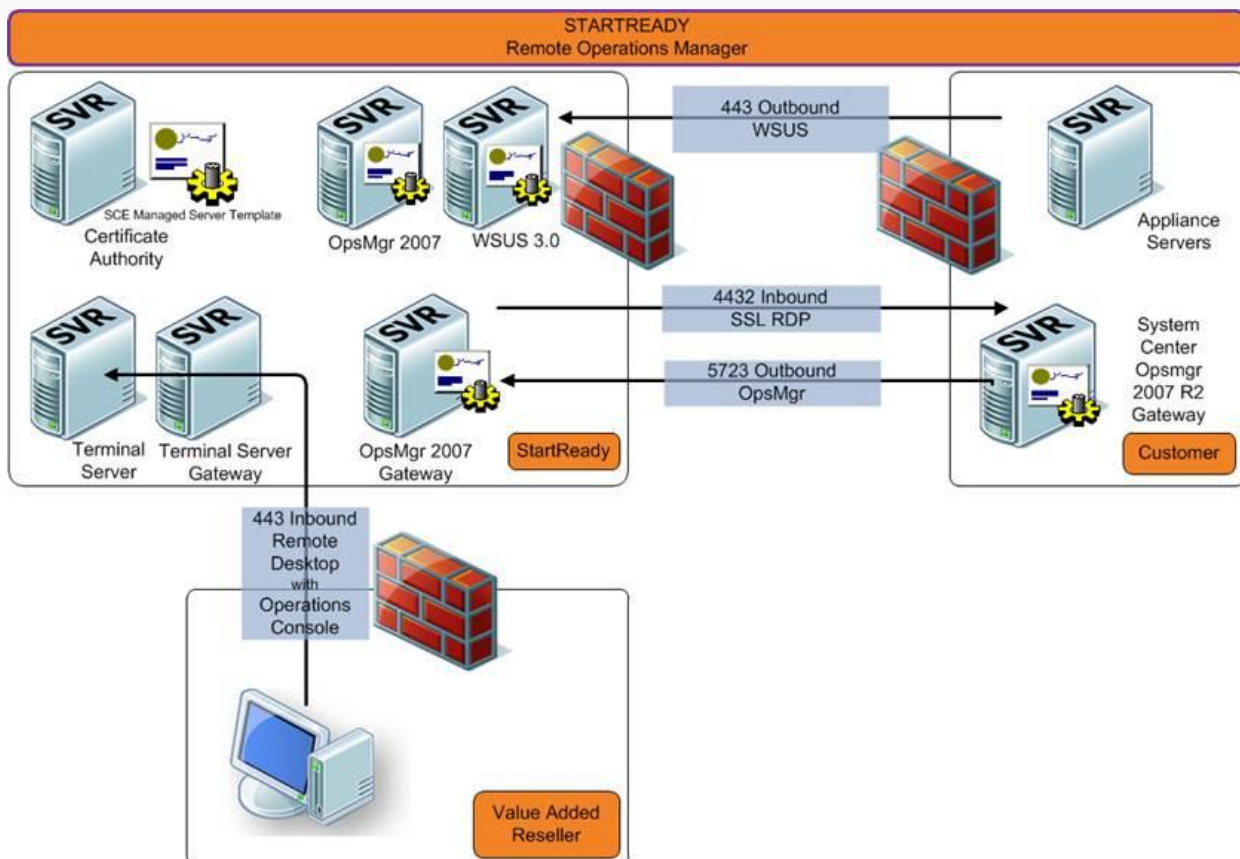


StartReady Appliances worden geïmplementeerd inclusief het volledig beheer. Hieronder verstaan wij 24x7 monitoring, remote ondersteuning, patch management en het borgen van de afgesproken SLA .

Tijdens een implementatie van een StartReady Appliance wordt de StartReady Management Server geïnstalleerd. De StartReady Management Server maakt gebruik van bestaande Microsoft technologieën voor het uitvoeren van de beheertaken:

- Remote toegang;
- Monitoring;
- Windows Updates.

Onderstaand architectuur overzicht schetst een beeld van de gebruikte software en communicatie.



### Remote toegang

Voor remote toegang maakt StartReady gebruik van een met SSL beveiligde Remote Desktop Sessie. De communicatie tussen het data-center van StartReady en de Appliance bij de klant verloopt via de poort 4432. De communicatie wordt beveiligd met behulp van een SSL certificaat zodat deze communicatie niet “afgeluisterd kan worden”. Bij de klant verwachten wij dan ook dat de poort 4432 wordt opengezet voor communicatie vanaf startready.com. Deze poort kan dus heel specifiek worden opengezet voor het toestaan van communicatie vanaf alleen startready.com of het bijbehorende IP-adres. Toegang voor onze partners wordt geregeld via onze omgeving.

### Monitoring

Om de afgesproken SLA te kunnen borgen vindt er 24\*7 pro-actieve monitoring plaats van alle StartReady Appliances. Op iedere server wordt een monitoring agent geïnstalleerd die er voor zorgt dat over de geleverde Microsoft (Lync) Software gegevens over het presteren worden doorgegeven aan de StartReady Monitoring omgeving. De management server, een virtuele server, op de appliance fungeert hiervoor als doorgeefluik. De doorgegeven gegevens komen via onze Operations Manager Gateway binnen in System Center Operations Manager (SCOM). SCOM zorgt met behulp van de Microsoft Management Packs voor de analyse en waarnodig voor de signalering aan de StartReady Support desk. De benodigde communicatie hiervoor verloopt via poort 5723 van de klant naar het datacenter van StartReady.

### Microsoft Updates

StartReady neemt de volledige verantwoordelijkheid voor het up-to-date houden van de geleverde Microsoft Software op de Appliance. Het up-to-date houden gaat op basis van de updates die vrijgegeven worden door Microsoft via Windows Update. De software geleverd op een StartReady Appliance verwijst naar een WSUS omgeving van StartReady. De benodigde communicatie hiervoor verloopt via 443 over het internet.

Door dit te doen kan StartReady de vrijgekomen Microsoft updates eerst zelf testen in zijn eigen teststraat. De teststraat bestaat uit een interne test en een test bij een pilot groep klanten. Indien dit succesvol is verlopen wordt de update vrijgegeven aan alle Appliances. De WSUS omgeving op de Appliance zal zijn catalogus in sync houden met de StartReady WSUS omgeving en indien er updates zijn vrijgegeven zullen deze worden gedownload bij Microsoft. Als er een reboot nodig is zal dit standaard om drie uur 's nachts worden uitgevoerd.

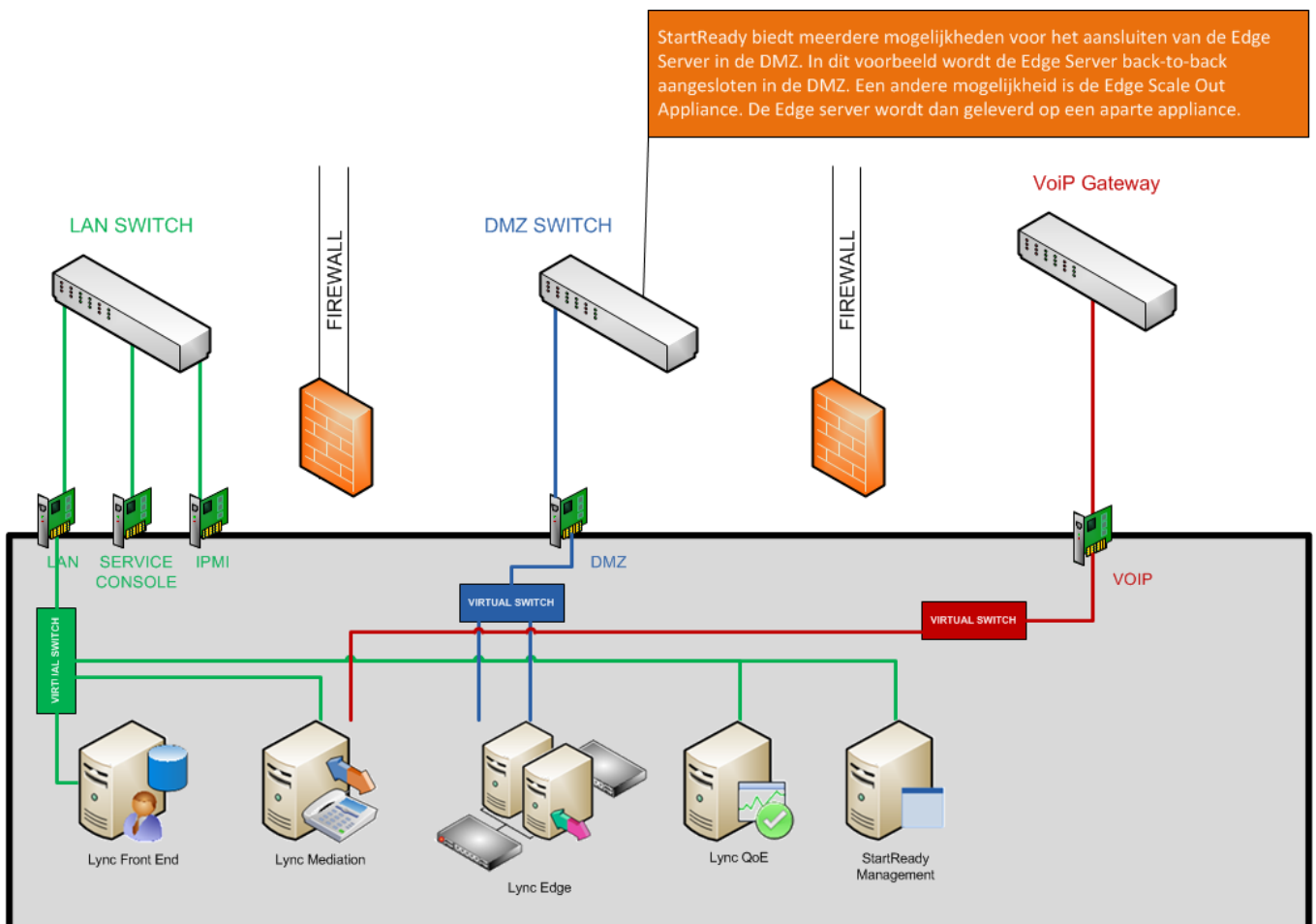
## StartReady Appliance in de IT infrastructuur.

Het aansluitschema toont zowel de fysieke netwerk aansluitingen als de virtuele netwerk aansluitingen. De fysieke aansluitingen worden aangesloten op de verschillende netwerksegmenten:

1. LAN (Local Area Network)
2. Management LAN (dit is optioneel voor bijvoorbeeld het service console en/of de IPMI interface)
3. DMZ (Demilitarized zone)
4. VoIP Gateway. Deze mag ook in de DMZ, maar dan mag de firewall geen NAT toepassen)<sup>1</sup>

De virtuele netwerkaansluitingen worden via de fysieke netwerkaansluitingen aangesloten op de virtuele servers in de Appliance.

Hieronder wordt een aansluitschema besproken van een Lync Appliance. Als voorbeeld is gekozen voor Appliance aangesloten op een SIP Trunk. Als er gekozen wordt voor een andere vorm van telefonie integratie kan de VOIP aansluiting iets wijzigen.



<sup>1</sup> Het SIP protocol ondersteunt geen NAT (Network Address Translation). Indien wel NAT wordt toegepast zal de oplossing niet naar behoren functioneren.

In totaal zijn er 5 fysieke netwerk aansluitingen:

1. LAN – Deze netwerkaansluiting sluit via de virtuele switch alle virtuele servers aan op het LAN van de infrastructuur.
2. Service Console – Deze netwerkaansluiting sluit de fysieke appliance aan op het LAN of optioneel op het Management LAN.
3. IPMI – Deze netwerkaansluiting sluit de IPMI (Intelligent Platform Management Interface) aan op het LAN of optioneel op het Management LAN. IPMI wordt gebruikt voor eventuele ondersteuning indien de fysieke server via de “normale” interfaces niet meer te benaderen is.
4. DMZ – Deze netwerkaansluiting sluit via de virtuele switch de “Lync Edge” aan op de DMZ. De “Lync Edge” is een Lync Server rol die de communicatie verzorgt met externe aansluitingen op internet. Dit kunnen thuisgebruikers, klanten of gefedereerde organisaties zijn.
5. VOIP – Deze netwerkaansluiting sluit via de virtuele switch de “Lync Mediation” aan op de SIP Trunk Provider. Deze aansluiting moet transparant zijn en mag dus niet via NAT aangesloten zijn op de Appliance.