Tjänstebeskrivning
Nätverk som tjänst

Leverantören tillhandahåller nätverk som en tjänst för nätverksenheterna i kundens nätverk.

Innehåll

1 Översikt

Leverantören tillhandahåller ett skalbart nätverk som en tjänst som uppfyller kundens prestanda-, tillgänglighets- och tillväxtbehov, samt ansvarar för övervakning och hantering av den tilldelade kapaciteten.

Vid nätverk som en tjänst betalar kunden bara för den kapacitet man faktiskt använder, och slipper tidskrävande upphandlingar och dyra investeringar. Leverantören tar ansvar för tillhandahållande och utveckling av tjänsten, så att kunden i stället kan fokusera på sin verksamhet.

När kundens behov förändras kan kapaciteten enkelt minskas eller ökas, och nya tjänster läggas till. På så sätt ser vi till att IT-miljön inte är ett hinder vid nödvändiga förändringar i verksamheten.

2 Tjänsteinnehåll och uppgifter

2.1 WLAN-tjänst

Med WLAN-tjänsten får företagen ett säkert och flexibelt, trådlöst, lokalt nätverk som komplement till befintligt LAN. Implementeringen av tjänsten kan variera från en miljö med en accesspunkt till en nätverkslösning bestående av flera hundra accesspunkter.

Lösningen bygger på leverantörens centrala WLAN-lösning.
Leverantören ansvarar för systemets tillgänglighet samt underhåll och hantering.

Övervakningen av tjänsten är aktiv dygnet runt.

WLAN-tjänsten täcker förändringar i konfigurationen av kundens WLAN-tjänst och dokumentation av ändringarna. WLAN-tjänsten och hanteringen av incidenter är aktivt vardagar kl. 8-17.
Hantering av incidenter avseende dedikerade konfigurationer utförs under tjänstens servicetider.

2.1.1 Innehåll och uppgifter

WLAN-tjänsten implementeras via ett separat, fysiskt WLAN-nätverk, där vi definierar logiskt åtskilda enheter som servar önskade användargrupper.

Nätverket är öppet och annonseras via radioöverföringsvägen till alla slutenheter

- Nätverksåtkomsten begränsas inte till radiointerfacenivå
- Klienter som är anslutna till nätverket måste autentiseras innan de får tillgång till internet. Autentiseringen hanteras normalt av en så kallad captive portal.

Ett WCS-system (Wireless Control System), som ingår i tjänsten, informerar automatiskt om eventuella avvikelser och nätavbrott. Med WCS kan ändringar i konfigurationerna och systemuppdateringarna göras från en plats.

Accesspunkterna justerar automatiskt frekvenskanalerna, för att inte störa varandra. Vid fel på accesspunkten ökar lokalens andra accesspunkter automatiskt sin överföringskapacitet, för att minimera den trasiga accesspunktens skuggzon. Funktionen kräver att det finns tillräcklig täckningsöverlappning mellan angränsande accesspunkter.

2.1.2 Tillval

Enligt kundens behov kan WLAN-tjänsten kompletteras med andra trådlösa nätverk, som annonseras med sina egna SSID-namn i samma fysiska WLAN-nätverk.

Andra WLAN kan vara:

- Företagsnätverk:
  - Ett slutet nätverk som inte annonseras i radions överföringsväg (dolt SSID)
  - Nätverksåtkomsten är begränsad och kräver autentisering enligt kundens angivna metoder (EAP-TLS, PEAP, WPA/WPA2-PSK etc.)
  - Radioöverföringsvägar som krypteras med TKIP- eller AES-algoritmer i enlighet med WPA/WPA2-standarden
  - Den trådlösa nätverksanslutningens slutpunkt är placerad antingen direkt i kundens LAN eller centralt i kundens datacenters nätverk
- BYOD-nätverk:
  - Ett internetanslutet nätverk för BYOD-enheter och andra enheter där det inte är önskvärt att ofta behöva autentisera enheten interaktivt via webbläsare.
  - Godkännandet tillhandahålls på radionivå genom en statisk nyckel i stället för autentisering via en s.k. captive portal.

- Leverantören kan beställa en nätverksanslutning mellan kundens nätverk och leverantörens datacenter. När det gäller installationen och månadsvgifterna följer priset för nätverksanslutningen den valda operatörens prissättning.
- Leverantören kan erbjuda övervakning och hantering av kundägt trådlöst LAN, enligt överenskommelse. Övervakning och hantering utförs i enlighet med leverantörens beskrivning av tjänsten nätverkshantering.

2.1.3 Separat debiterade uppgifter

Kunden kan till exempel beställa följande tjänster från leverantören:

- Täckningsmätningar, s.k. site survey, i kundens lokaler och tillhörande rapportering
- Att till tjänsten ansluta extra utrustning

2.1.4 Begränsningar och ansvar

Leverantören ansvarar för design och genomförande av tjänsten inom de gränser som anges i denna beskrivning.

Kunden ansvarar för:

- Godkännande av radio-LAN implementeringsplan
- Utse en kontaktperson inom den egna organisationen, för hela planerings- och implementeringsfasen
- Informera och handleda användarna i den egna organisationen
- Organisera och genomföra uppdatering av arbetsstationer, tillsammans med leverantören
- Leverera dokument som krävs för design- och implementeringsarbetet till leverantörens tekniker, t.ex. planritningar
- Se till att leverantörens tekniker får tillgång till kundens anläggning efter behov
- Aktivera anslutningen av mätutrustning i kundens nätverk
- Konfigurering av LAN- och brandväggsinställningar, när nätverket inte ingår i leverantörens övervaknings- och hanteringstjänst
- Tjänsten kräver en nätverksanslutning mellan leverantörens datacenter och kundens nätverkssegment. Kunden ansvarar för nätverksanslutningen samt upphandlingen och de löpande kostnaderna, om inte annat avtalas.

Tjänsten täcker endast design av WLAN-nätverket och dess anslutning till LAN. Design av kundens IP-plan och virtuellt LAN sker endast i den mån detta krävs för WLAN-nätverket.

Leverantören ansvarar inte för eventuella störningar i det radiospektrum som det trådlösa nätverket använder.

2.1.5 Rapportering

Den grundläggande rapporteringen innehåller enhetsspecifik tillgänglighet (SLA) under överenskomna servicetider.
Vad gäller andra rapporter avtalas de från fall till fall.

2.1.6 Aktiviteter vid initiering

Tjänsten initieras som en del av utrullningsprojektet eller som ett separat uppdrag. Tjänstens initiering omfattar:

- Installation av utrustning (accesspunkter) i kundens lokaler
- Anslutning av utrustningen till leverantörens övervakningssystem
- Förberedelse av enhetsspecifik kommunikation och arbetsinstruktioner
- Dokumentation av komponenter i leverantörens inventariehanteringssystem
- Förberedelse av riktlinjer för kontinuerlig tjänst

2.1.7 Ändringar

Leverantören äger rätt att ändra tjänstens tekniska miljö utan att avtala detta med kunden. Däremot måste ändringar som påverkar kundens tjänst alltid avtalas med kunden.

2.1.8 Aktiviteter efter uppsägning

Vid uppsägning av tjänsten kommer leverantören demontera åtkomstpunkterna från kundens lokaler, koppla ur kunden från servicenätverket och avlägsna kundens nätverkskomponenter från systemen. Leverantören överlämnar all servicerelaterad, kundspecifik dokumentation till kunden.

Vid migrering av tjänsten till kund eller tredje part, debiterar leverantören för de timmar som går åt till migreringsarbete.
Initiering av migreringsarbetet utförs som ett separat uppdrag eller som ett överenskommet migreringsprojekt.

2.1.9 Teknik som stöds

Som ett minimum har leverantören stöd för utrustning från följande hårdvarutillverkare:

- Cisco
- Meru

2.1.10 Debiteringsmodell

Tjänsten debiteras per åtkomstpunkt som ingår i tjänsten, per månad.

2.1.11 Tjänstens tillgänglighet

Bastjänstens tillgänglighet (SLA), utom underhållsfönster och enstaka AP-fel, är 99,7 % per månad.

2.2 Internettjänst

Internettjänsten är ett abonnemang som ansluter kundens LAN och offentliga servrar till internet från leverantörens datacenter. Kundens LAN-segment och servrar finns i leverantörens datacenter, eller också är kundens LAN-segment eller delar av det anslutet till leverantörens datacenter, och nätverksanslutningar replikeras till internetåtkomstpunkter.

Leverantören ansvarar för internetabonnemangets kapacitet och tillgänglighet, samt övervakning och hantering, vilket leverantören utför med hjälp av egen övervaknings- och hanteringsprogramvara samt metoder och processer.

2.2.1 Innehåll och uppgifter

Internettjänsten levereras som en internetansluten nätverkspunkt, som ansluter till Fujitsus AS (Autonomous System). Därefter kan enheter anslutas till nätverkspunkten, som en fysisk eller virtuell enhet. När det gäller fysiska enheter ses en port som internetanslutningspunkt.

Tjänsten medger internetanslutning för olika ändamål, via Fujitsus eget internetstamnät. Fujitsus internettjänst har dubbla globala IP-transiteringar som garanterar optimal prestanda och tillgänglighet.

Åtkomstalternativen är, per punkt, 10, 100 eller 1000 Mbps, och kan skalas upp eller med fasta konfigureringar, allt efter behov.

2.2.2 Tillval

Kunden kan även få tillgång till följande tilläggstjänster:

2.2.2.1 IP-subnätrouting

Som standard tillhandahåller leverantören ett antal fasta IP-adresser i ett subnät. Det här alternativet förändrar implementeringen så att ett Fujitsu-tilldelat eller kundägt nätverk kan styras om via ett transportnätverk till kundens router. För det här alternativet tas en engångsavgift ut.

2.2.2.2 Kundägt subnät

Om kunden vill annonsera sitt eget leverantörsoberoende (Provider Independent - PI) adressutrymme och använda det för konnektivitet, kan Fujitsu annonsera det i den globala BGP-routingtabellen från Fujitsus AS. För det här alternativet tas en engångsavgift och en månadsavgift ut.

2.2.3 DNS-tjänst

DNS-tjänsten består av följande:

- Leverantören ansvarar för registreringen av domänerna, utifrån kundens önskemål
- Leverantören ansvarar för domänernas synlighet och relaterade data i det publika nätet (auktoriserade namnservrar)
- Domänunderhåll (lägga till, ändra och ta bort datanamn och ip-detaljer)
- Underhåll, övervakning och hantering av namnservern
- Problemhantering
- Övervakning av domännamnens (som är täckta av tjänsten) utgång samt återaktivering
- Leverantören ansvarar för kostnaderna för domänregistrering och domänregistreringsförnyelse
- Separat debiterade tilläggstjänster
  - Registrering av nytt domännamn
  - Tillägg av nytt domännamn

2.2.4 Separat debiterade uppgifter

Leverantören kan, för kundens räkning, utföra en bedömning av nödvändiga förutsättningar för tjänstens initiering, även kallat analys av tjänstemiljön. Det här är en expertuppgift som debiteras separat.

2.2.5 Begränsningar och ansvar

Kunden ansvarar för:

- Upprätthålla datasäkerhetspolicyn och se till att tilldelade datakommunikationsprocesser följer datasäkerhetspolicyn
- Se till att ingen hårdvara eller mjukvara som används av kunden kan orsaka skador eller avbrott för leverantören eller andra internetanvändare
- Tjänsten kräver en nätverksanslutning mellan leverantörens datacenter och kundens nätverkssegment. Kunden ansvarar för nätverksanslutningen samt upphandlingen och de löpande kostnaderna, om inte annat avtalas.

2.2.6 Rapportering

På begäran kan kunden få en trafikrapport som visar mängden trafik via gränssnittet.

2.2.7 Aktiviteter vid initiering

Vid tjänsteinitiering kommer leverantören att

- Ställa in en nätverkspunkt som passar den anslutna enheten.
- Tilldela IP-adresser.

- Ställa in IP-routing (om alternativet IP-subnätrouting har valts).
- Skapa/uppdatera routeobjekt och se till att subnätannonseringen syns i den globala routingtabellen (om alternativet kundägt subnät har valts).

2.2.8 Ändringar

Leverantören äger rätt att ändra tjänstens tekniska miljö utan att avtala detta med kunden. Däremot måste ändringar som påverkar kundens tjänst alltid avtalas med kunden.

2.2.9 Aktiviteter efter uppsägning

Fujitsu bryter åtkomsten till de nätverkspunkter som ingår i tjänsten och upphör att annonsera kundspecifika nätverk. I förekommande fall kan Fujitsu hjälpa kunden eller tredje part att ta över ansvaret för eventuella kundspecifika RIPE-objekt från Fujitsu. Tänk på att Fujitsu-ägda IP-adresser och IP-nätverk inte kan överlåtas.

2.2.10 Tjänstens tillgänglighet

SLA är 99,95 % per månad för Internet Core. För att varje system ska nå denna tillgänglighet, måste nätverket anslutas med dubbla, redundanta anslutningar. Enkla anslutningar har en SLA på 99,7 %.

2.3 Brandväggstjänst

Brandväggstjänsten levereras i form av en brandväggshantering, där Fujitsu tar allt ansvar för drift, underhåll, övervakning och hantering. Tjänsten medger finkornig trafikfiltrering mellan nätverken.

Det finns även fler valbara funktioner, som medger terminering av VPN-användare och fjärranslutning av kontors-VPN. Förstärkt tillgänglighet och säkerhet kan också läggas till, med hjälp av valbara tilläggstjänster.

2.3.1 Förutsättningar

För att abonnera på den här tjänsten måste nedanstående lista över förutsättningar vara uppfylld, annars kan inte Fujitsu leverera tjänsten.

Förteckning över förutsättningar:

- Ett tillgängligt nätverk i Fujitsus DC.
- En fördefinierad implementeringsplan som omfattar IP-adressering, filtreringsregler, autentiseringskällor etc.

2.3.2 Funktioner som ingår

Den här listan presenterar de funktioner som ingår i tjänsten.

Lista över funktioner som ingår:

- En brandvägg som gör finkorniga filtreringar av IP-trafiken, med två tillgängliga gigabit ethernetgränssnitt.
- Övervakning och hantering.
- Support för hård- och mjukvara.
- Hantering av problem och incidenter

2.3.3 Tillval

Följande alternativ kan läggas till, mot extra kostnad.

2.3.3.1 Support för fjärranslutet kontors-VPN

Det här alternativet innebär att brandväggen kan terminera IPSec VPN från fjärrstyrda kontor med brandvägg i andra änden, med tunnlar för hela subnät. I alternativet ingår inga tjänster på fjärrenheten och tillgänglighets-SLA gäller inte på VPN-anslutningar, på grund av att infrastrukturen ligger utanför Fujitsus kontroll. Det här alternativet faktureras som en fast månadsavgift, plus en extra månadsavgift per konfigurerad VPN-tunnel.

2.3.3.2 Support för fjärranvändar-VPN

Med det här alternativet kan brandväggen terminera VPN-anslutningar från fjärranvändarenheter, för att användarnas enheter ska kunna komma åt nätverk och resurser bakom brandväggen. Användarenheterna

måste både kunna använda och stödjas av den programvara som tillhandahålls av Fujitsu. Användarna autentiseras med hjälp av en extern autentiseringskälla (RADIUS eller LDAP – ingår inte i tjänsten), plus ett OTP (One-Time Password - engångslösenord) som levereras till användarnas mobiltelefoner. Det här alternativet faktureras som en fast månadsavgift, plus en extra månadsavgift per aktiv användare. En aktiv användare är ett konto som har använts minst en gång under faktureringsperioden.

2.3.3.3 Kluster för ökad tillgänglighet

Det här alternativet ger två brandväggar som konfigureras som ett brandväggskluster, vilket ökar tjänstens tillgänglighet. Alternativet faktureras som två tjänstekomponenter, plus en extra månadsavgift för båda komponenterna.

2.3.3.4 IDS-kapacitet

Med det här alternativet kan brandväggen fungera som en IDS, genom att använda funktioner som upptäcker skadlig trafik. Tillsammans med övervakning och eskalering ger tjänsten möjlighet till att både manuella och automatiska skyddsåtgärder görs.

2.3.3.5 Antivirus och filtrering av internettrafik

Det här alternativet möjliggör skanning av HTTP-trafik i syfte att förebygga åtkomst till vissa webbplatser och webbplatskategorier. Här finns även funktioner för antivirusskanning i realtid, av potentiellt skadligt innehåll från webbplatser.

2.3.4 Aktiviteter vid initiering

Vid tjänsteinitiering kommer leverantören att

- Tillhandahålla nödvändig hårdvara
- Installera och konfigurera hårdvara, mjukvarulicenser och funktioner som ingår i tjänsten*.
- Konfigurera övervakning och hantering.

* - Om det inte finns någon detaljerad implementeringsplan, eller om planen saknar all erforderlig information, förbehåller Fujitsu sig rätten att fakturera den extra tid som läggs på planering av implementeringen (arbetstid).

2.3.5 Aktiviteter efter uppsägning

Direkt efter mottagen skriftlig uppsägning avslutar Fujitsu åtkomsten till tjänsten. Fujitsu förbehåller sig rätten att debitera kunden för en extra månad efter att uppsägningen har mottagits. Eventuella ytterligare förfrågningar i samband med uppsägningen av tjänsten debiteras per timme (arbetstid).

2.3.6 Begränsningar och ansvar

Varje brandvägg har en maximal kapacitet på 1 Gbit/s. För snabbare konnektivitetsalternativ kan i stället en kundspecifik lösning förvärvas.

2.4 Lastbalanseringstjänst

Lastbalanseringstjänsten innebär att leverantören förvärvar och underhåller den lastbalanseringsutrustning som krävs. Tjänsten kan tillhandahållas med dedikerad lastbalanseringsutrustning eller via leverantörens delade lastbalanseringsutrustning.

Övervakningen och problemhanteringen för utrustningens plattform är aktiv dygnet runt.

I lastbalanseringstjänsten ingår förändringar i konfigurationen av kundens lastbalanseringsutrustning och dokumentation av ändringarna. Lastbalanseringstjänsten är aktiv vardagar kl. 8-17.
Problemhantering av dedikerade konfigurationer utförs under hanteringstjänstens servicetider.

Hanteringstjänster tillhandahålls fjärrstyrt från leverantörens datacenter.

2.4.1 Innehåll och uppgifter

Leverantören ansvarar för användbarhet, konfiguration och uppdatering av lastbalanseringsplattformen , samt miljöns informationssäkerhet.

Tjänsten täcker
- Konfiguration av tjänsten
- Dokumentation av miljön

2.4.2 Tillval

Bastjänsten stöder en kapacitet på 100 Mbit. Som alternativ finns uppgradering till 1 eller 10 Gbit.

2.4.3 Separat debiterade uppgifter

Arbete som utförs utanför ordinarie servicetider debiteras separat.

Separat debiterade uppgifter:
- Lägga till en ny enhet
- Lägga till en ny kontext
- Justera en befintlig kontext
- Ta fram optimeringsförslag som specialistarbete

2.4.4 Begränsningar och ansvar

Kunden ansvarar för:
- Att designa en backendinfrastruktur tillsammans med leverantören.

2.4.5 Rapportering

Leverantörens grundläggande rapportering täcker lastbalanseringsplattformens tillgänglighet (SLA) under överenskomna servicetider, inom ramen för tjänstemiljöns tillgänglighet.
Övriga rapporter avtalas från fall till fall.

Genom särskild överenskommelse kan följande övervakas och rapporteras:
- Tjänstens systembelastning

2.4.6 Aktiviteter vid initiering

Initieras som en del av projektinitieringen, eller som separat uppgift. Uppstartfasen innehåller, som ett minimum, följande:
- Design av lastbalanseringsmiljön tillsammans med kunden
- Val av lämplig lösning för förväntad lastkonfigurering av IP-adresser
- Konfigurering av lastbalansering
- Konfigurering av övervakning

2.4.7 Ändringar

Leverantören äger rätt att ändra tjänstens tekniska miljö utan att avtala detta med kunden. Däremot måste ändringar som påverkar kundens tjänst alltid avtalas med kunden.

2.4.8 Aktiviteter efter uppsägning

Vid uppsägning av tjänsten ska leverantören koppla ur kunden från servicenätverket och avlägsna kundens nätverkskomponenter från systemen. Leverantören överlämnar all servicerelaterad, kundspecifik dokumentation till kunden.

Vid migrering av tjänsten till kund eller tredje part, debiterar leverantören för de timmar som går åt till migreringsarbete.
Initiering av migreringsarbetet utförs som ett separat uppdrag eller som ett överenskommet migreringsprojekt.

.

2.5 802.1x-autentiseringstjänst

802.1x-autentiseringstjänst är ett säkert sätt att autentisera enheter som inte är anslutna till kundens nätverk. Tjänsten skyddar kundens LAN-nätverk (eller delar av det) från obehörig uppkoppling, vare sig det görs medvetet eller omedvetet.
802.1x-autentisering innebär att enheter som ansluter till kundens nätverk kan dirigeras till nätverksanslutningar och -resurser som i förväg har tilldelats användaren.

802.1x-autentiseringstjänsten kan tillhandahållas via autentiseringssystem som ägs antingen av kunden eller leverantören och som finns i kundens eller i leverantörens lokaler.

Leverantören ansvarar för kapaciteten och tillgängligheten hos 802.1x-autentiseringssystemet, som levereras som en tjänst, och licenser på 802.1x-autentiseringsprogram samt övervakning och hantering av systemet.

Övervakningen och problemhanteringen för utrustningens plattform är aktiv dygnet runt.

I 802.1x-autentiseringstjänsten ingår förändringar i konfigurationen av kundens autentiseringsutrustning och dokumentation av ändringarna.

Problemhantering av dedikerade konfigurationer utförs under hanteringstjänstens servicetider.

Hanteringen tillhandahålls fjärrstyrt från leverantörens datacenter.

2.5.1 Innehåll och uppgifter

Leverantören ansvarar för användbarhet, konfiguration och uppdatering av 802.1x-autentiseringstjänstens plattform som en resurs, samt miljöns informationssäkerhet.

Syftet med tjänstens funktioner är att tillhandahålla en säker anslutning till kundens nätverk. Autentiseringen förhindrar att icke tillförlitliga enheter kopplar upp sig till kundens nätverk, vare sig det sker medvetet eller omedvetet. Autentiseringen medger även olika typer av dynamiska nätverksanslutningar för olika användargrupper.

Som standard erbjuder tjänsten två olika anslutningsprofiler:

- Intranätanslutning (kräver 802.1x-autentisering av enheten)
  - Enheter anslutna till kundens Windows AD-domän
  - Andra tillförlitliga enheter
    - Skrivare
    - IP-kameror
    - WLAN-åtkomstpunkter

Autentiseringen baseras på 802.1x-autentisering av enhet som ansluts till nätverket. Autentiseringen använder X.509-certifikat. Behörig anslutning till kundens nätverk medges för enheter som har ett aktivt enhetscertifikat installerat och ett aktivt enhetskonto i kundens Windows-domän.

För tillförlitliga enheter som ansluts till nätverket och som inte stöder 802.1x-autentisering, utgår tjänsten utifrån MAC-adress (MAC Authentication Bypass, MAB).

- Internetanslutning (för enheter som inte passerar 802.1x-)
  - I första hand enheter som inte är tillförlitliga och som inte behöver ansluta direkt till kundens interna nätverk.
  - För besökare i kundens lokaler som inte är behöriga för kundens LAN-nätverk.

Enheter som inte stöder 802.1x-autentisering alls eller som inte klarar autentiseringen kan anslutas dynamiskt till internetanslutet nätverk med konnektivitet endast mot publika nät (internet).

Som tillval kan leverantören tillhandahålla fler anslutningsprofiler. Valbara anslutningsprofiler definieras mer i detalj tillsammans med kunden, under implementeringsprojektet.

Tjänsten täcker:

- Konfigurering av kundens dedikerade nätverksenheter
- Dokumentation av miljön

2.5.2 Tillval

Leverantören kan även erbjuda följande tjänster, som tillval till autentiseringstjänsten:

- 802.1x-autentisering för kundens WLAN-nätverk
- Leverantören kan även erbjuda övervakning och hantering av en kundägd 802.1x-autentiseringsplattform.

2.5.3 Separat debiterade uppgifter

Arbete som utförs utanför ordinarie servicetider debiteras separat.

Separat debiterade uppgifter:

- Lägga till en ny enhet
- Expansion av 802.1x-autentiseringstjänsten för kundens övriga kontor eller AD-domäner
- Skapa valfria anslutningsprofiler för 802.1x-autentiseringsmiljön
- Tredjepartssupport.

2.5.4 Begränsningar och ansvar

Kunden ansvarar för att:

- Kundens AD- och CA-miljöer finns i en servermiljö som kör Windows 2008 R2 eller nyare.
- Kunden har en befintlig PKI-miljö.
- Kundens arbetsstationsmiljö är baserad på Windows 7 eller nyare, och samtliga enheter som behöver autentiseras stöder 802.1x-autentisering.
- Nätverksanslutningar mellan leverantörens tjänstenätverk och kundens nätverk.
- Problemlösning av arbetsstationsmiljön (om Fujitsu inte tillhandahåller kundens arbetsstationsmiljö).

När det gäller 802.1x-autentiseringstjänsten antar vi att Fujitsu övervakar och hanterar kundens nätverksenheter (LAN/WLAN).

2.5.5 Rapportering

Leverantörens grundläggande rapportering täcker 802.1x-autentiseringsplattformens tillgänglighet (SLA) under överenskomna servicetider, inom ramen för tjänstemiljöns tillgänglighet.
Övriga rapporter avtalas från fall till fall.

2.5.6 Aktiviteter vid initiering

Initieras som en del av projektinitieringen, eller som separat uppgift. Uppstartfasen innehåller, som ett minimum, följande:

- ACS/ISE-plattformens konfiguration
- Konfigurering av Radius-programvara
- Konfigurering av 802.1x-parametrar till switcharna
- Konfigurering av AD GPO-parametrar (om AD-tjänsten tillhandahålls av Fujitsu)
- Konfigurering av CA-tjänstens parametrar
- GPO-distribution till arbetsstationerna

2.5.7 Ändringar

Leverantören äger rätt att ändra tjänstens tekniska miljö utan att avtala detta med kunden. Däremot måste ändringar som påverkar kundens tjänst alltid avtalas med kunden.

2.5.8 Aktiviteter efter uppsägning

Vid uppsägning av tjänsten ska leverantören stänga av kunden från servicenätverket och avlägsna kundens nätverkskomponenter från systemen. Leverantören överlämnar all servicerelaterad, kundspecifik dokumentation till kunden.

Vid migrering av tjänsten till kund eller tredje part, debiterar leverantören för de timmar som går åt till migreringsarbete.

Initiering av migreringsarbetet utförs som ett separat uppdrag eller som ett överenskommet migreringsprojekt.

2.5.9 Tjänstens tillgänglighet

SLA är 99,7 % per månad, utom planerat underhåll.

2.5.10 Teknik som stöds

Ett minimum säger att leverantören stöder komponenter från följande hårdvarutillverkare:

- Cisco (802.1x-autentiseringsplattform och switchar)

.

2.6 WAN Services

2.6.1 Mål och Syfte

Målet med Tjänsteelementet WAN Service är att möjliggöra pålitlig kommunikation mellan kundens lokaliteter och centrala Data Center samt säkerställa att dataöverföringens/kommunikationens funktion, prestanda och tillgänglighet är på en nivå i paritet med, eller överstigande, överenskomna tjänstenivåer.

2.6.2 Generell beskrivning

WAN är den funktionalitet som möjliggör kommunikation mellan Kundens geografiskt spridda lokaliteter och Leverantörens anslutningspunkter till relevant(a) Data Center, och därmed tillhandahåller slutanvändarna konnektivitet till centralt placerad infrastruktur samtidigt som fjärrmanövrering av infrastruktur placerad hos kund möjliggörs.

WAN Service levereras enligt genom att tillhandahålla en helhetslösning vilken omfattar leveranshantering, inklusive administration, uppföljning och integration genom tredjepartsleverantör som ansluter kundens definierade lokaliteter.

2.6.3 Managed WAN Service (WAN Hanteringstjänst)

Leverantören är ansvarig för upprätthållande av tjänsten via avtal med tredjepartsleverantör av WAN tjänster med avseende på kundens och den egna verksamhetens WAN som tillhandahåller kommunikation mellan alla lokaliteter och områden. Leverantören säkerställer hantering av tredjepartsleverantören av WAN-tjänsten så att denne lever upp till sitt ansvarsåtagande relaterat till leveransen.

2.6.3.1 Quality of Service (Kvalitetsnivå för tjänst) – (Tillvalstjänst)

Managed WAN Service kan som option, och föremål för separat debitering, konfigureras med kvalitetssäkring/prioritering av nätverkstrafik (s.k. QoS: Quality of Service) för att garantera tillgänglig bandvidd mellan specifika applikationer, protokoll eller enheter. Prioriteringen kategoriseras i följande nivåer;

- Premium – Högt prioriterad kommunikation; t.ex. VoIP (röstsamtal över IP)
- Express – interaktiva applikationer; t.ex. snabbmeddelanden, SSH
- Standard – kommunikation som inte behöver prioriteras
- Bulk – Låg prioritet, t.ex. nerladdningar

Behovet av QoS för kunden analyseras och definieras i samarbete mellan parterna för att säkerställa att rätt förutsättningar är uppfyllda och att inga tekniska begränsningar hindrar införandet, samt att målen med tjänsten kan uppfyllas.

2.6.3.2 WAN Acceleration – (Tillvalstjänst)

Managed WAN Service kan som option, och föremål för separat debitering, konfigureras att nyttja WAN-acceleration för att på så sätt öka effektiviteten i dataöverföringar. Leverantören tillhandahåller teknisk infrastruktur, inklusive underhåll och support, för denna tjänst och administrerar tjänsten via leverantörsspecifika verktyg och applicerbara optimeringstekniker.

Behovet av WAN-acceleration för kunden analyseras och definieras i samarbete mellan parterna för att säkerställa att rätt förutsättningar är uppfyllda och att inga tekniska begränsningar hindrar införandet, samt att målen med tjänsten kan uppfyllas.

3 Tjänstens livscykel

3.1 Aktiviteter vid tjänsteinitiering

Tjänster kan initieras antingen individuellt eller i grupper som separata projekt. En tjänst initieras i enlighet med leverantörens egen process. Initieringsarbetet specificeras i ett övergångsprojekt.

Leverantören utser en person som ansvarar för tjänsteinitieringen. En projektinitiering kan brytas ned i flera delprojekt, beroende på miljöns storlek och antalet förändringar. Delprojekten kan till exempel omfatta teknisk migrering, initiering av nätverksdriftens servicecenter, diverse utvärderingar, analyser samt vägledning och eventuell utbildning.

Kunden kommer att, i erforderlig utsträckning, delta i tjänsteinitieringen och se till att kundens systemleverantörer och andra tredje parter bidrar till en framgångsrik tjänsteinitiering.

Initieringen godkänns och bedöms som färdig efter gemensamt beslut av kund och leverantör.

En ansvarsmatris tas fram i samband med tjänsteinitieringen, där alla ansvariga personer förs in.

Om inte annat har avtalats separat börjar tjänsten debiteras så snart den, eller en del av den, har överlämnats till kunden.

3.2 Ändringar i tjänsten

Leverantören äger rätt att ändra tjänstens tekniska miljö utan att avtala detta med kunden. Däremot måste ändringar som påverkar kundens tjänst alltid avtalas med kunden.

3.3 Aktiviteter efter uppsägning av tjänst

När tjänsten sägs upp ska allt som finns registrerat i tjänstebeskrivningen, samt tjänster som kan kopplas till detta avtal och dess leverans, demonteras, kunddata raderas och användandet av alla tjänsterelaterade verktyg avbrytas. En gemensam uppsägningsplan tas fram, som innehåller följande:

- Kommunikation
- Avlägsnandet av användarkonton från leverantörssystemen
- Avlägsnande av dokumentation
- Avlägsnande av tjänstehanteringssystem och andra eventuella system
- Leverans av data som har lagrats av leverantören för kunds räkning (t.ex. register över tillgångar) samt eliminering av kunddata från tjänsteobjekt
- Återkallande av rapporteringsprocessen
- Demontering av anslutningar för datakommunikation
- Överlämning av uppgifter avseende finansiering till kunden

3.4 Underhållsfönster

Leverantören förbehåller sig rätten till ett underhållsfönster, varunder servicemiljön inte är tillgänglig. Underhållsfönstret schemaläggs till den första och tredje söndagen i varje månad, klockan 03-07. Leverantören underrättar kunden om underhållsfönstret senast fem arbetsdagar före det schemalagda datumet. Leverantören kan även, vid tvingande skäl, uppdatera miljön vid andra tider (t.ex. omfattande säkerhetshot).

Alla tjänster i det här dokumentet delar samma underhållsfönster.