

peelit SECURITY SATELLITE

Peelit Security Satellite är en ny lösning för säker fjärraccess till bland annat säkerhets- och fastighetssystem. Lösningen ger användarna full tillgång till geografiskt spridda system från valfri punkt, via stationära eller mobila klienter. Peelit Security Satellite bidrar därför till ökad kontroll, förenklad administration och lägre kostnader för användarna.

Användning:

Satelliterna lämpar sig för företag med flera separata LAN som till exempel butikskedjor eller tillverkningsföretag med flera fabriker. Eftersom satelliterna är förkonfigurerade och kan hyras på månadsbasis så är de även en utmärkt lösning för att bygga IT-infrastruktur på tillfälliga anläggningar som byggarbetsplatser.

Exempel på system som kan anslutas är brand- och inbrottslarm, fil- och databasservrar, processtyrningsutrustning, HVAC-system, CCTV och mycket annat. Lösningen fungerar utmärkt med integrerade säkerhets- och styrsystem, exempelvis AppVision.

Med hjälp av definierade roller kan tillgången till olika system regleras. Exempelvis kan operatörer begränsas till att bara ha tillgång till system som är direkt relevanta för deras uppgifter och utomstående supportpersonal kan få tidsbegränsat tillträde för underhåll eller felsökning av enbart sina levererade delsystem. Drift och administration kan därför utföras både enklare och säkrare eftersom åtkomsten segmenteras.

Satelliterna baseras på hårdvara från AppGate eller Cisco och ansluts till Peelits eller kundens egna datacenter via krypterad uppkoppling. De kan hyras eller köpas vilket ger stor flexibilitet.

Välkommen att kontakta oss för mer information eller för att själva testa på konceptet!

0730 – 84 84 00

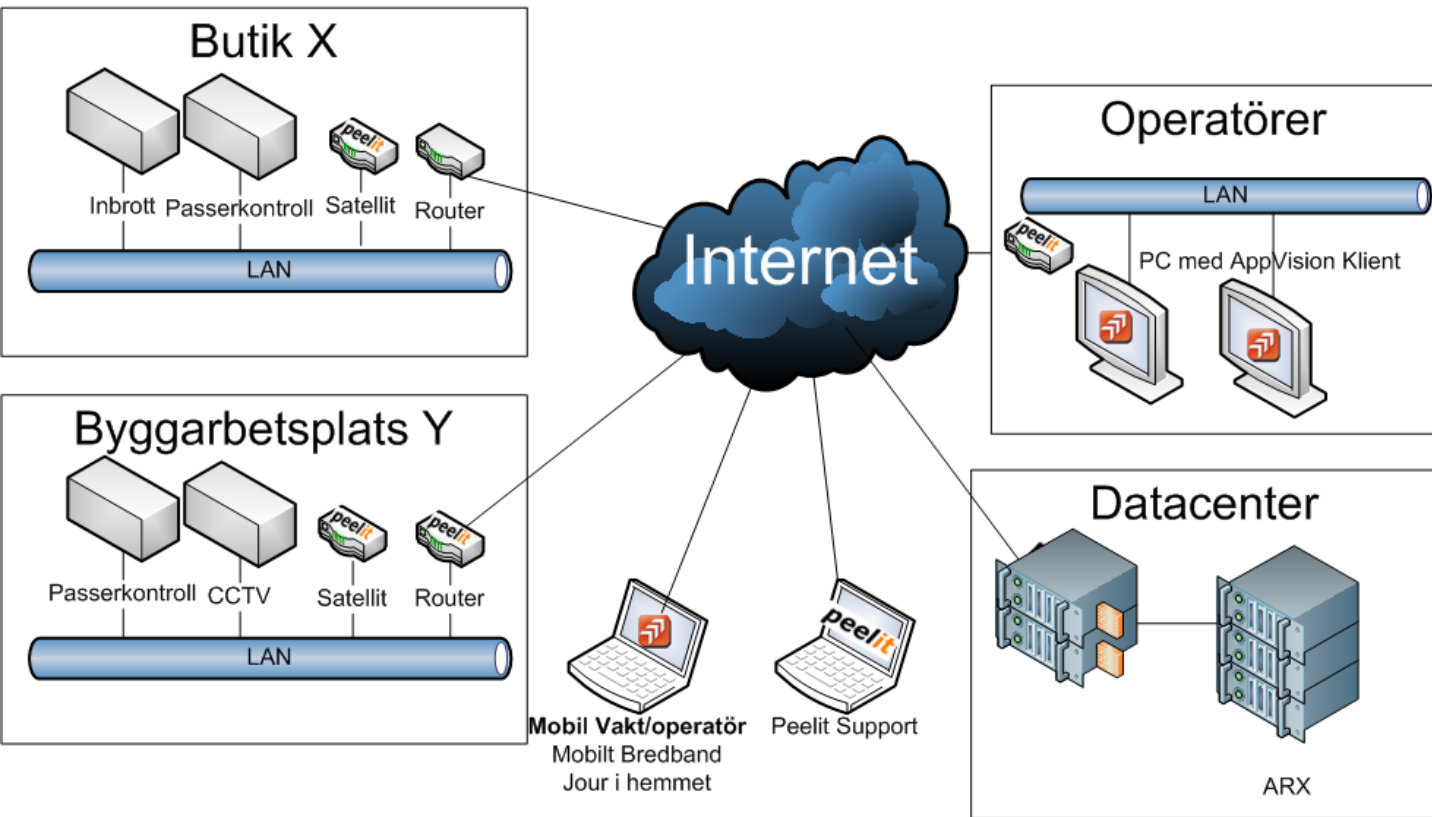
info@peelit.se

peelit

appGATE™
NETWORK SECURITY

CISCO

Teknik



Tekniken bygger på en central säkerhetsserver som agerar proxy för all kommunikation såväl mot internet som mellan LAN:ets delsystem. Satelliterna sköter kommunikationen med säkerhetsservern och ansluts till de olika spridda nätverk som användaren vill ha fjärråtkomst till. Access och identifiering kan då hanteras från en central punkt. All trafik krypteras end-to-end med 128-bitars kryptering.

Om ett delsystem komprometteras så minskar även risken för att andra system påverkas, eftersom delsystemen inte står i direkt kontakt med varandra. Strukturen möjliggör en segmentering av de olika delsystemen på nätverken, vilket skapar ett djupledsförsvar. Via stark tvåfaktorsautentisering för all påloggning så förstärks även identitetskontroll och rättighetshantering.