

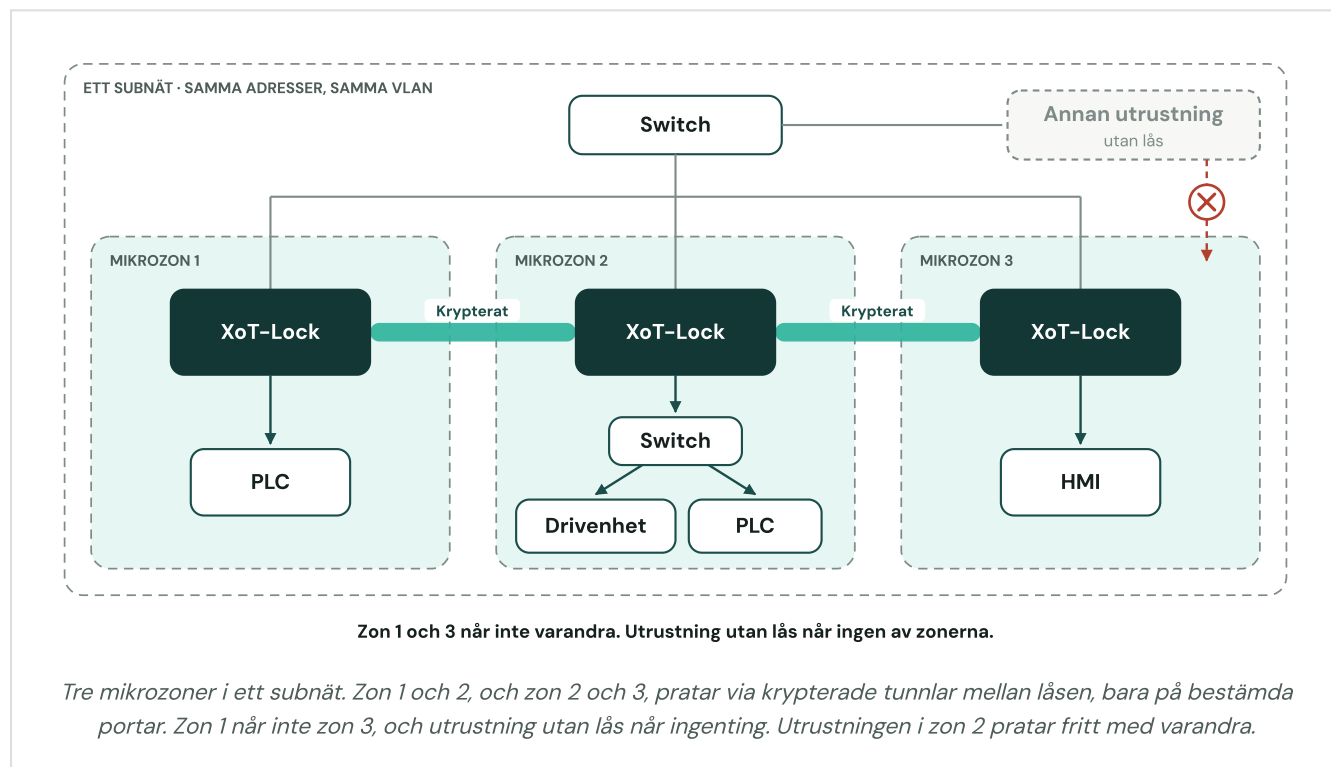
GUIDE I SJU STEG

Mikrosegmentering med Hide and Protect

Guiden beskriver en metod i sju steg. Med den delar ni upp ett befintligt nätverk i mikrozoner med XoT-Lock och licensen Hide and Protect. Reglerna i XMS styr trafiken mellan zonerna. Utrustningen behåller IP-adress, VLAN och inställningar, och metoden minskar risken för stopp i produktionen. En mikrozon kan gå över flera subnät och VLAN. Den kan också ligga inne i ett enda subnät.

01 Målbild

Varje mikrozon sitter bakom ett eget lås i transparent läge. Allt nekas från början. Tillåten trafik mellan zonerna går i krypterade tunnlar mellan låsen, och bara på bestämda portar. Bilden visar ett exempel: mikrosegmentering inne i ett enda subnät.



02 Metoden i korthet



Steg 1 och 2 görs vid skrivbordet. Steg 4 och 5 är en tillfällig period då ni lär er trafiken. Ingen trafik stoppas förrän i steg 7.

03 Steg för steg

1 Förteckna utrustningen

Vet exakt vad som finns i nätverket

- **Förteckna all utrustning** i nätverket som ska delas upp: IP-adress, MAC-adress, funktion, tillverkare och vem som sköter den.
- **Bedöm hur kritisk den är.** Vilken utrustning är sårbar, gammal eller viktig för säkerheten? Den får det starkaste skyddet.
- **Använd det som redan finns:** nätverksritningar, MAC-tabeller i switcharna, konfigurationen i SCADA och tillverkarnas dokumentation.
- **Bestäm hur utrustningen ska klassas** i reglerna: Asset Type och Asset Group (vad) samt Country, City, Address och Room (var).

RESULTAT

En förteckning över utrustningen, med taggar.

2 Hitta lager 2-domänerna

Bestäm mikrozonerna

- **Bara IP-trafik passerar ett lås.** Protokoll på lager 2 gör det inte. Leta upp utrustning som pratar med varandra på lager 2, till exempel med PROFINET RT eller IEC 61850 GOOSE.
- **Placera sådan utrustning bakom samma lås**, till exempel via en liten switch på låsets DEVICE-port.
- **Allt annat får en egen zon.** Helst har varje enhet ett eget lås.
- **Kom ihåg:** trafik mellan utrustning i samma zon passerar inte låset. Den filtreras alltså inte.

RESULTAT

En karta över zonerna. Den visar vilken utrustning som sitter bakom vilket lås och hur många lås som behövs.

- **Planera varje lås egen adress:** IP-adress, gateway, DNS och NTP. Kontrollera att låset når XMS på TCP 443 via NETWORK-porten.
- **Installera låset i transparent läge:** NETWORK-porten till den befintliga switchen och DEVICE-porten till utrustningen eller cellens switch.
- **Registrera varje lås** i XMS. Lägg in den skyddade utrustningen som tillgångar, med taggarna från steg 1.
- **Utrustningen behåller** IP-adress, nätmask, gateway och VLAN.

RESULTAT

Registrerade lås och tillgångar i XMS.

VIKTIGT Låset nekar allt från början. Ett lås utan aktiv regel släpper inte igenom något. Skapa därför regeln som tillåter allt (steg 4) innan låset sätts in. Ni kan också göra båda i samma servicefönster.

- **Skapa en tillfällig regel** för varje lås som tillåter all trafik: alla avsändare, alla mottagare och alla portar och protokoll.
- **Ge regeln ett tydligt namn** som visar att den är tillfällig, och skriv in ett datum. Då glöms den inte bort.
- **Kontrollera** att processen fungerar precis som innan låsen sattes in.

RESULTAT

Låsen är på plats, och driften fungerar som förut.

- **Slå på Traffic Discovery** i varje lås. Låset registrerar varje flöde med avsändare, mottagare, portar och protokoll. Uppgifterna skickas till XMS.
- **Registrera en hel driftcykel:** alla skift, alla batcher, veckojobb som säkerhetskopiering och servicetillfällen med leverantörer.
- **Ovanliga händelser är viktigast.** Ett flöde som bara sker en gång i månaden blir annars stoppat senare.

RESULTAT

En lista över trafiken för varje enhet: vem den pratar med, på vilka portar och hur mycket.

6 Analysera och skapa regler

Ge bara den behörighet som behövs

- **Utrustning** → **utrustning i en annan zon** → regel mellan två lås (klientens lås → serverns lås) på exakt de portar som behövs.
- **Personer** (operatörer, tekniker, leverantörer) → regler för användargrupper via XoT-Desktop Client eller XoT-WebAccess. Gör dem tidsbegränsade när det går.
- **Utrustning** → **system utanför låsen** (historian, SCADA, server för uppdateringar) → utgående regel, helst till en registrerad Unprotected Asset.
- **Okända eller oväntade flöden** → utred dem innan ni tillåter dem. Alla flöden som syns behövs inte.
- **Granska reglerna** med driften och dem som äger utrustningen innan reglerna börjar gälla.

RESULTAT

Granskade regler, sparade men inte aktiva (Inactive).

7 Aktivera reglerna

Neka allt som inte är tillåtet

- **Planera ett servicefönster** och ta en zon i taget. Börja med den minst kritiska.
- **Aktivera zonens regler och ta bort regeln som tillåter allt** för den zonen.
- **Kontrollera driften** med den som ansvarar för processen innan ni går vidare till nästa zon.
- **Återställning:** spara regeln som tillåter allt som Inactive. Då kan ni aktivera den igen på några sekunder.

RESULTAT

Ett nätverk i mikrozoner, med dokumenterade zoner och regler.

04 Regler som gäller hela tiden

- ☐ **Licens:** mikrosegmentering kräver licensen Hide and Protect för varje skyddad maskin. Med bara Remote Access är låset i öppet läge. Då kan det inte stoppa trafik i det lokala nätverket eller begränsa utgående trafik.
- ☐ **Kapacitet:** krypteringen begränsar hur mycket trafik ett lås klarar. Planera för stora flöden mellan zonerna, och använd mjukvarulåset för de största.
- ☐ **Tid:** regler mellan maskiner är permanenta. Regler för personer gäller en begränsad tid.
- ☐ **Support:** er partner ger support i första hand. Vid svårare frågor får partnern hjälp av Xertified.

MYCKET VIKTIGT XMS, NTP-servrar och DNS-servrar får aldrig läggas in som skyddade tillgångar. De får inte heller vara mottagare i någon regel, inte ens när de finns i samma subnät. Låset har en enda routingtabell, och trafiken för administrationen måste gå utanför tunnlarna.