Identitetsbaserad åtkomstkontroll för uppkopplade enheter.

Den saknade biten i säkerheten för IT, OT och IoT. Policy Graph, tillfällig åtkomst, Traffic Discovery, WebAccess, spegling av trafik och avgränsad administration.

INNEHÅLL

Fjorton funktioner i ert system med XoT technology.

01	Skydd utan att ändra nätet	03
02	Mikrosegmentering inom ett subnät	04
03	Regler: åtkomstkontroll i XoT	05
04	Tillfällig åtkomst	06
05	Godkännande av åtkomst	07
06	Policy Graph visar säkerhetsläget	08
07	Kontroll av regeln med inbyggd graf	10
08	Traffic Discovery, med rapport skriven av AI	11
09	WebAccess	13
10	XoT-Desktop Client	15
11	Administratörer med avgränsat ansvar	16
12	Spegling av trafik	17
13	XoT-Bridge	18
14	Skyddat hela vägen	19



Sätt ett lås framför en tillgång. Den behåller IP-adress, gateway och VLAN.

01 **Sätt låset i trafikvägen**

Mellan switchen och enheten. Inget ändras i själva tillgången.

02 **Samma adress på båda sidor**

Tillgången behåller IP-adress, gateway och VLAN. Resten av nätet når den som förut.

03 **Osynlig tills en regel tillåter**

Från det att låset sitter på plats når bara trafik som en regel tillåter fram till tillgången.

Byggt för äldre OT

Enheter som inte kan konfigureras om eller uppdateras får skydd där de står. Inget driftstopp, inga nya IP-adresser.

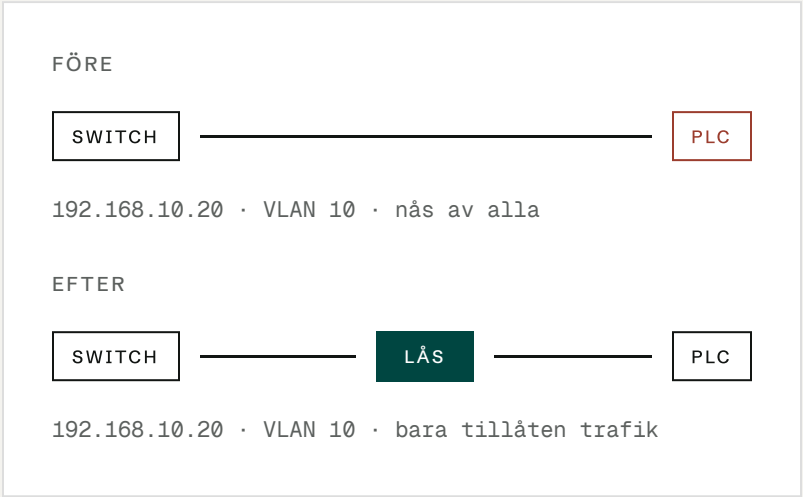


Fig. 1 Samma adress, nu skyddad. Bara tillåten trafik passerar låset.

Isolera en enhet eller en grupp i samma subnät, utan att röra nätets uppbyggnad.

01 **Ett lås per enhet eller grupp**

Framför en enda enhet, eller framför en grupp som ska behandlas som ett segment.

02 **Regeln avgör vem som pratar med vem**

Förbindelser från lås till lås (M2M) tillåts per port och protokoll. Allt annat i subnätet blockeras.

03 **Inga nya IP-adresser, inga nya VLAN**

Det platta nätet förblir platt. Bara förtroendemodellen ändras.

Stoppar rörelser i platta nät

En arbetsstation som tagits över når inte längre PLC:erna bredvid.

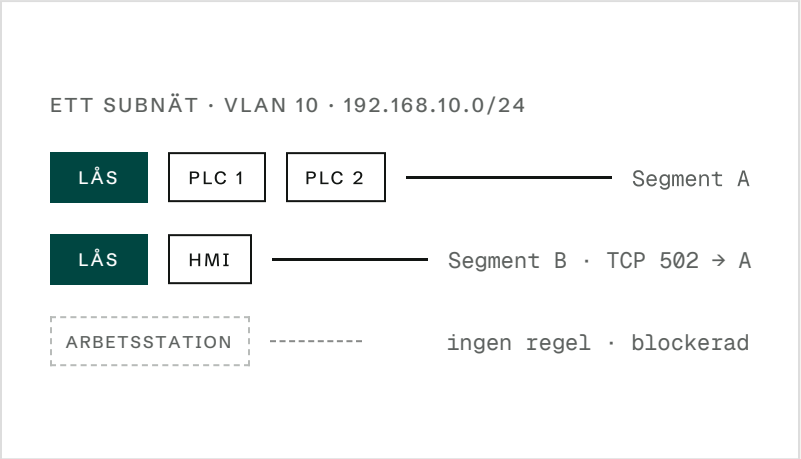


Fig. 2 Regel: HMI → PLC-gruppen, bara på TCP 502. Arbetsstationen delar subnät med dem men når ingen av dem.

Vem som når vad, hur och när. Inga IP-adresser behövs.

KÄLLA

Vem

Användargrupper från er identitetskälla, eller maskiner efter typ och plats.

TRAFIK

Hur

Bara tillåtna portar och protokoll. Allt annat nekas.

MÅL

Vad

Tillgångar efter typ och plats. Egenskaper, inte IP-adresser.

EXEMPEL PÅ REGEL

SUPERUSER · GRUPP — FJÄRRÅTKOMST TILL PLC — PLC #34 · STOCKHOLM · CELL 34

TCP 502 · torsdag 09.00–13.30 · från EWS-klienten, Stockholm

Tillfällig från grunden

Regler kan ha en tidsgräns, gälla en gång eller återkommande, och kan kräva godkännande av en utsedd administratör.

Ingen stående åtkomst. Ges enligt schema eller efter godkännande och upphör av sig själv.

NEDRÄKNING

Tidsgräns från aktivering

Gäller en bestämd tid och upphör sedan automatiskt. Till exempel fyra timmar från aktivering.

EN GÅNG

Ett bestämt fönster

Gäller ett visst datum, mellan bestämda start- och sluttider. Till exempel ett servicefönster.

ÅTERKOMMANDE

Upprepas automatiskt

Upprepas enligt schema och är stängd mellan fönstren. Torsdagar 09.00–13.30, varje vecka.

VID GODKÄNNANDE

På begäran

Ges per begäran av en administratör och upphör sedan. Mer på nästa bild.

Inga stående behörigheter

Oavsett om åtkomsten är schemalagd eller godkänd per begäran är den stängd från början och upphör av sig själv. Det minskar attackytan kraftigt.

Tillfällig åtkomst med en människa som godkänner.

ADMIN

Skapar regel

Tillgångar märks så att utvalda användare kan begära åtkomst.

ANVÄNDARE

Begär åtkomst

Skäl och tid, eller antal timmar från godkännandet.

GODKÄNNARE

Granskar begäran

Får ett mejl med begäran och skälet. Avslag skickas tillbaka med ett skäl.

ANVÄNDARE

Sessionen är aktiv

Regeln aktiveras och tunneln är öppen under det godkända fönstret.

ANVÄNDARE

Sessionen slutar

Upphör vid sluttiden eller avslutas i förtid av godkännaren.

Begärd, godkänd, tidsbegränsad, stängd

Den som begär och de som godkänner får mejl vid varje ändring och innan en begäran eller session går ut. Aldrig öppen längre än nödvändigt.

Vem som når vad och genom vilken regel, läst ur den sparade konfigurationen.

01 **Fråga åt båda hållen**

Vem kan nå en viss enhet, eller vad kan den här användaren eller gruppen nå?

02 **Få svaret som en graf**

Varje väg ritas: användare → grupp → regel → tillgång. Inget gissas.

03 **Kontrollera ert säkerhetsläge**

Hitta för höga behörigheter, oväntade vägar och bortglömda regler. Visa revisorn bevisen (NIS2, IEC 62443).

Visar alla regler i systemet

Aktiva, schemalagda och inaktiva regler ritas. Inget döljs.

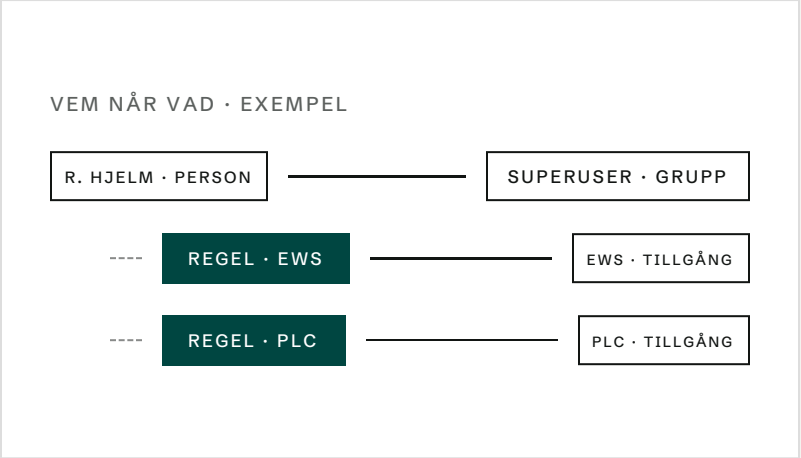


Fig. 3 En användare, en grupp, två regler, två tillgångar. Fyra verkliga exempel på nästa bild.

Fyra frågor som en revisor ställer, var och en besvarad med en bild.

FRÅGA

Vad har Rikard Hjelm åtkomst till?

Två tillgångar, EWS och PLC, båda via gruppen SuperUser.

FRÅGA

Vem har åtkomst till EWS-systemet?

Sju användare via två regler, bland dem alla konsulter.

FRÅGA

Vem har åtkomst till SCADA?

Två användargrupper och EWS-klienten. Alla vägar och regler i en vy.

FRÅGA

Vad når gruppen Konsulter?

PLC, SCADA HMI och EWS, alla via Consultant Access.

Se vad en regel skulle omfatta, innan något sparas eller börjar gälla.

Samma graf visas medan du bygger en regel. Access Overview visar vad regeln skulle omfatta om den sparades som den är.

01 Alla användare i källgruppen

02 Alla tillgångar som typ och plats matchar

03 Uppdateras direkt när du ändrar ett fält



Fig. 4 Access Overview ritar grafen medan du fyller i regeln.

Se vad en skyddad tillgång verkligen pratar med. Skriv sedan en regel som tillåter just det.

01 **Fånga trafiken i låset**

Varje flöde genom ett lås registreras på 5-tupelnivå och skickas till XMS.

02 **Läs det i XMS**

Grupperat per skyddad enhet: vilka värdar den pratar med, på vilka portar och hur mycket data.

03 **Låt AI skriva rapporten**

Exportera flödena till ett AI-verktyg för en rapport på vanlig svenska och förslag på regler.

Från okänt till minsta behörighet

Börja med en tillfällig regel som tillåter allt, kartlägg den verkliga trafiken och ersätt sedan regeln med avgränsade regler.

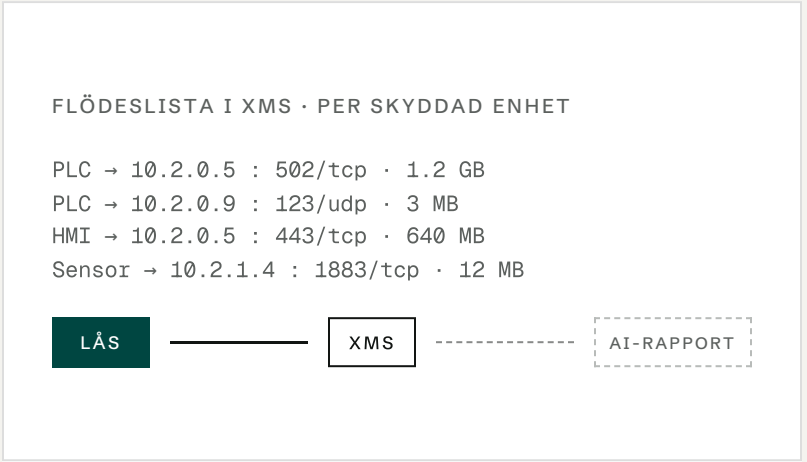


Fig. 5 Allt till allt under kartläggningen, avgränsade regler när den är klar.

Exportera flödena från XMS och få en rapport till ägaren av tillgången.

01 **Flödeskarta per lås**

Vilka skyddade enheter som pratar med vilka värdar, portar och protokoll. Ritat, inte listat.

02 **Sammanställda flöden**

En rad per källa, mål och tjänst, med datamängd och antal paket.

03 **Iakttagelser och förslag**

Iakttagelser på vanlig svenska och regler med minsta behörighet, klara att skapa i XMS.

Använd er egen AI. Ingår inte i XoT.

Rapporten tas fram av ett externt AI-verktyg som ni själva väljer. XoT exporterar bara flödesdata. AI-modellen, lokalt eller i molnet, är er egen.

EXEMPELRAPPORT · FRÅN ETT EXTERNT AI-VERKTYG

Sida 1 · sammanfattning och flödeskarta
Sida 2 · flöden och iakttagelser

TREDJE PART · INTE XoT

Åtkomst till skyddade tillgångar via webbläsaren. Inget att installera på användarens enhet.

01

Logga in

Webbläsaren ansluter till WebAccess-servern. Samma IdP, MFA och inloggning som i XMS.

02

Eget skrivbord

En Debian-container per användare startar vid behov och strömmas till webbläsaren. Inga tillägg.

03

PKI per session

Nya certifikat från XMS, giltiga bara för den här sessionen, används av Desktop Client i containern.

04

Tunnel till låset

Biljett, åtkomstbegäran och WireGuard-tunnel, precis som en vanlig klient. Reglerna gäller fullt ut.

Inspelning av sessioner

Varje session i WebAccess kan spelas in på skärmen. Det ger ett fullständigt spår av vad som gjordes med skyddade tillgångar.

Begränsad till sessionen

När sessionen slutar raderas containern och dess inloggningsuppgifter. Inget finns kvar på enheten.

HTTPS till WebAccess. WireGuard från containern till låset.

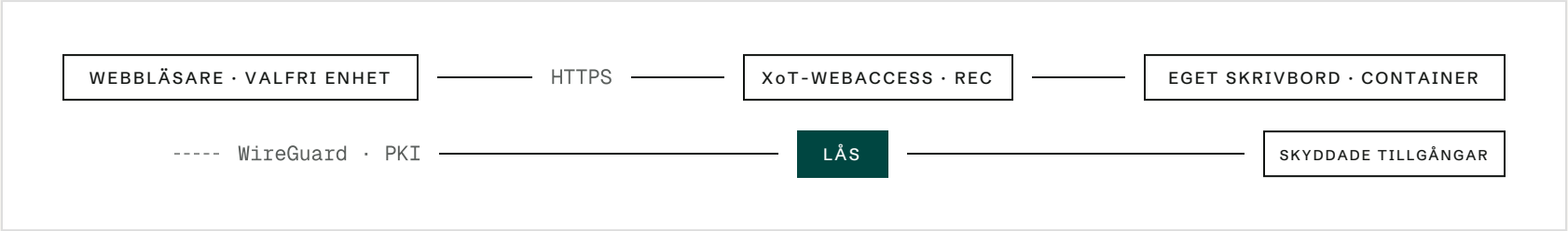


Fig. 6 Webbläsaren ansluter till WebAccess över HTTPS med IdP:n i XMS. Från containern går en WireGuard-tunnel med PKI-autentisering till låset, med samma biljett, åtkomstbegäran och regel som alla klienter.

En klient för alla användare. Er egen inloggning och ert val av lagring för nyckeln.

01 **Installeras en gång och fungerar sedan**

Pekar på er XMS, eller förkonfigureras via Intune eller MDM. Tunnlarna öppnas så fort en regel är aktiv.

02 **Loggar in via er IdP**

Lösenord, MFA eller det er identitetsleverantör kräver. Användare och grupper från LDAP eller Entra ID.

03 **Den privata nyckeln sparas där ni vill**

Nyckeln signerar den utmaning och det svar som körs inne i varje tunnel, två gånger i minuten.

Utan skärm för servrar

Samma klient körs som en systemtjänst utan grafiskt gränssnitt. Samma inloggning, tunnlar och regler.

HÄR LIGGER ANVÄNDARENS PRIVATA NYCKEL

Nyckel i fil	TPM i datorn	Hårdvarunyckel
Sparas som en fil på datorn. Snabb att rulla ut, inget extra att köpa.	Låst i datorns TPM. Bunden till den datorn, kan inte kopieras.	På en YubiKey eller ett smartkort. Innehav + PIN. Högsta säkerhet.

BEKVÄMLIGHET — SÄKERHET

Alla tre fungerar med samma regler, biljetter och tunnlar. Valet görs per användare eller grupp, inte för hela systemet.

Varje administratör sköter bara sin egen anläggning eller kund. En XMS, delad administration.

01 **Ett ansvarsområde är en del av XMS**

Lås, tillgångar och regler som hör till en anläggning eller kund.

02 **Full kontroll inom området**

Registrera lås, skapa tillgångar och regler, bara i det egna området.

03 **Bara läsrätt utanför**

Andra områden och globala inställningar kan visas men inte ändras. Bara superadmin sköter allt.

Byggt för MSP:er och organisationer med många anläggningar

En XMS betjänar många kunder eller anläggningar, med en strikt gräns för vem som får ändra vad.



Fig. 7 Ingen administration mellan områdena.

Varje paket som passerar låset kopieras till era verktyg för övervakning och djup analys.

01 **Hela paketet speglas**

Huvud och innehåll, precis som de passerade låset. Inte en sammanfattning eller en flödespost.

02 **Levereras till er mottagare**

En SIEM, IDS/IPS eller inspelningsserver i ert nätverk får kopian i realtid.

03 **Byggt för djup analys**

Djup paketinspektion, kriminalteknisk analys och upptäckt av avvikelser i OT-protokoll på verklig trafik.

Kompletterar Traffic Discovery

Traffic Discovery visar flödena i XMS. Speglingen ger era säkerhetsverktyg hela paketen.

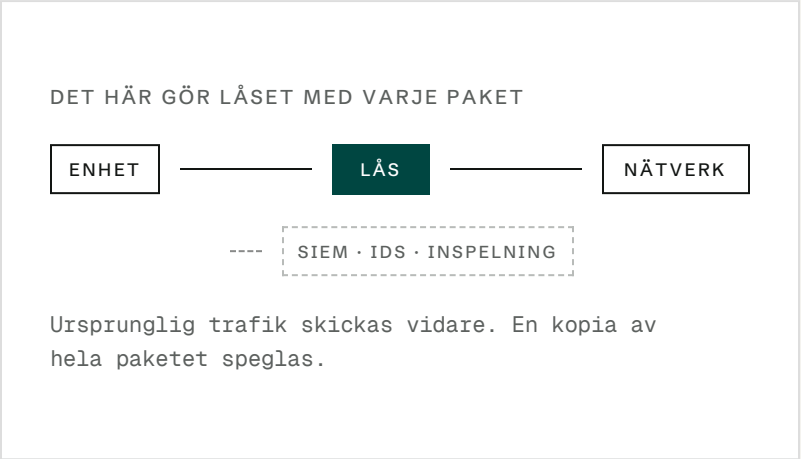


Fig. 8 Trafiken skickas vidare och en fullständig kopia speglas.

Nå lås bakom brandväggar utan att öppna en enda inkommande port.

01 **Bara utgående**

Klienter utifrån och lås inifrån ansluter båda ut till bryggan. Inga regler för inkommande trafik, någonstans.

02 **En ingång, hundratals lås**

Placeras i molnet eller i en DMZ med publik IP. Ett nytt lås kräver aldrig mer en ändring i brandväggen.

03 **Ser aldrig era data**

Skickar WireGuard-tunneln vidare utan att dekryptera den. Har en egen PKI-identitet, och alla klienter autentiserar sig mot den.

Gjord för Remote Access

Bryggan och låset i programvara är samma program i olika lägen.

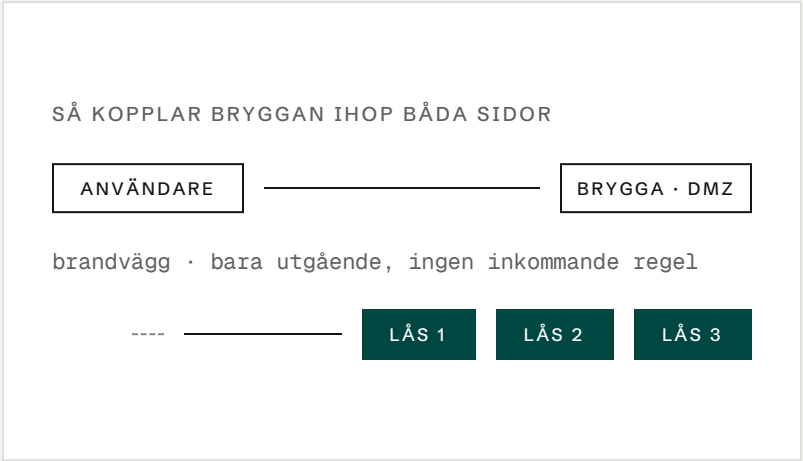


Fig. 9 Klientens tunnel slutar i bryggan. En andra WireGuard-tunnel går vidare till låset. Biljetten försöker nå låset direkt först och går via bryggan om det inte går.

Varje komponent har en kryptografisk identitet. Varje förbindelse är autentiserad och krypterad.

01 **PKI-identitet för allt**

Lås, klienter, brygga och XMS har var sitt certifikat från den inbyggda CA:n eller er egen. Inga delade hemligheter.

02 **WireGuard för all åtkomsttrafik**

Ömsesidig PKI-autentisering i åtkomstbegäran, sedan en WireGuard-tunnel. Utmaning och svar två gånger i minuten.

03 **Secure MQTT för administration**

En MQTT-session skyddad med certifikat till XMS på port 443. Regler, biljetter och driftdata går bara där.

Nollförtroende, kryptografiskt bevisat

Inget får förtroende för att det sitter på en viss plats i nätet. Identiteten bevisas i varje steg.

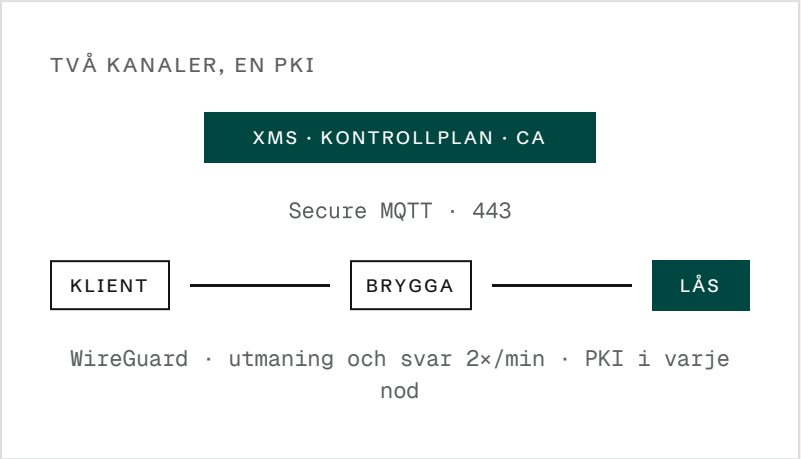


Fig. 10 Administration över Secure MQTT, åtkomsttrafik över WireGuard. PKI-identitet med certifikat i varje komponent.

Allt som är uppkopplat kan nås. Fram till nu.

SALES@XERTIFIED.COM · +46 (0)18 265 06 06