

# Axpo Group utilizza SecureTrack™ per il Firewall Operations Management



### L'azienda

Axpo Group è un'azienda svizzera leader nel settore della fornitura di energia. Grazie alle proprie centrali situate nella regione nordorientale e centrale della Svizzera, Axpo genera ogni giorno l'elettricità necessaria per oltre tre milioni di persone.

Dal 2001 Axpo Informatik fornisce servizi informatici di carattere tecnico e commerciale ai membri del gruppo Axpo e ai suoi clienti. Axpo Informatik ha la propria sede centrale a Baden e cinque uffici regionali ad Aarau, Beznau, Dietlikon, Schaffhausen e Zurigo. Attualmente l'azienda, grazie ad un'organizzazione estremamente sofisticata, serve 3500 utenti in tutta Europa e gestisce oltre 500 applicazioni.

Oltre ad occuparsi una vasta gamma di sistemi aziendali, logistici e operazionali, Axpo Informatik offre assistenza al sistema commerciale per la Svizzera, la Francia, l'Italia e l'Austria. Questi sistemi devono imperativamente beneficiare dei più elevati livelli di sicurezza e accessibilità.

### L'ambiente

Poiché il numero dei clienti di Axpo Group è in costante aumento, è necessario che la sicurezza sia gestita in maniera flessibile e rapida. Per questo l'azienda ha deciso di rendere virtuali parti fondamentali della propria infrastruttura di server e firewall, riuscendo così a implementare e fornire nuovi servizi in maniera rapida senza compromettere la sicurezza. Questo cambiamento ha consentito ad Axpo di ridurre sensibilmente i tempi necessari per la realizzazione di un firewall per i nuovi clienti. Axpo Informatik aveva bisogno di una soluzione in grado di gestire un'architettura sia fisica che virtuale.

L'infrastruttura firewall esistente è basata su un Crossbeam X40 Cluster ridondante con Check Point VPN-1 Power VSX. La gestione del firewall comprende un server centrale Check Point Provider-1 con un log server dedicato che permette di servire 10 clienti con 29 sistemi firewall fisici e virtuali. I sistemi critici sono configurati come hot standby cluster. I collegamenti della rete da e verso il sistema Crossbeam sono basati sulle tecnologie VLAN e Multilink Trunk.

## La sfida

Mantenere in efficienza e far funzionare 29 firewall con numerosi oggetti e rule base implica molto lavoro manuale e ripetitivo. Ogni volta che viene eseguita una modifica, gli operatori devono stabilire quali clienti e rule base sono implicati, quindi aggiornare manualmente ogni oggetto all'interno di ciascuna rule base. Inoltre in questo caso molti clienti utilizzavano la stessa infrastruttura, moltiplicando così rischi e complessità. Con tre amministratori di firewall era quindi molto difficile tenere traccia di ogni modifica alla configurazione e analizzarne l'impatto sulla sicurezza. In pratica era diventato quasi impossibile garantire la sicurezza e l'uniformità dei database degli oggetti e delle rule base.

Mentre la piattaforma di gestione esistente era caratterizzata da una configurazione centralizzata, Axpo Informatik aveva bisogno di un'approccio più uniforme e "dall'alto verso il basso". La soluzione ideale doveva consentire di rispondere rapidamente alle esigenze dei clienti assicurando contemporaneamente il coordinamento e l'approvazione di ogni modifica.

## La soluzione

Axpo Informatik ha scelto Tufin SecureTrack per ottenere una visione d'insieme completa dei criteri del firewall di tutti i clienti e di tutti gli oggetti. L'interfaccia grafica unificata di SecureTrack consente agli amministratori di visualizzare i criteri del firewall, comprendere le modifiche e intraprendere le azioni necessarie con la massima semplicità.

Il sistema di gestione delle modifiche del firewall di SecureTrack ha fornito una risposta efficace all'esigenza di Axpo Informatik di garantire affidabilità e uniformità poiché consente la registrazione e la segnalazione di ogni modifica in tempo reale. SecureTrack ha consentito ad Axpo

Informatik di individuare violazioni e possibili falle nella sicurezza prima che si potessero verificare dei danni confrontando sistematicamente ciascun cambiamento con gli standard aziendali predefiniti.

Poiché le rule base erano estremamente complesse e difficili da mantenere efficienti, Axpo Informatik ha iniziato a utilizzare le funzioni di ottimizzazione e cleanup di SecureTrack per individuare e rimuovere le regole e gli oggetti inutilizzati. Così gli addetti al firewall hanno potuto eliminare possibili falle nella sicurezza e al tempo stesso migliorare notevolmente le prestazioni e l'utilizzo delle risorse hardware. Le innovative funzioni di analisi di cui dispone SecureTrack hanno consentito ad Axpo Informatik di comprendere la logica della rule base e di semplificare i complessi criteri di sicurezza del firewall.

Poiché Axpo Group è un'azienda pubblica, le caratteristiche di auditing e conformità di SecureTrack hanno costituito un ulteriore punto di forza, garantendo la massima affidabilità, una registrazione completa per l'audit e il rispetto di importanti normative e standard internazionali.

SecureTrack è stato installato e seguito Clounet, azienda svizzera leader nell'integrazione dei sistemi. "Installare SecureTrack è stato molto semplice. In sole due ore il prodotto era già completamente operativo. Successivamente Axpo Informatik ha installato autonomamente un aggiornamento; entrambi siamo rimasti estremamente soddisfatti dell'assistenza di Tufin" dichiara Christen Martin, socio di Clounet. "Axpo, dopo aver valutato altre soluzioni, ha scelto SecureTrack perché unisce in un unico prodotto la capacità di operare in tempo reale e una grande semplicità di utilizzo".

## I vantaggi

"Dopo alcuni mesi SecureTrack ha modificato considerevolmente il funzionamento del firewall di Axpo, aiutandoci a ridurre le interruzioni del sistema e i tempi di inattività della rete. Adesso sappiamo esattamente quali modifiche vengono fatte da chi e SecureTrack ci consente di analizzare le nostre rule base per diversi firewall in qualsiasi momento".

David Spale  
Security Officer, Axpo Informatik

"Adesso passiamo meno tempo ad aggiornare manualmente tutti i nostri firewall e possiamo quindi dedicarci maggiormente ai nostri clienti. L'automatizzazione garantita da SecureTrack ha reso il nostro team più efficiente".

Bühler Werner  
Team Manager, Network &  
Security Services, Axpo Informatik

I vantaggi offerti da SecureTrack ad Axpo:

- Maggiore sicurezza della rete
- Un aumento dei tempi di operatività della rete e del servizio
- Minori costi di gestione
- Implementazione delle linee guida aziendali per la sicurezza
- Gestione del rischio
- Continuità nell'attività commerciale
- Conformità con le normative relative al settore informatico
- Miglioramento delle prestazioni del firewall
- Applicazione proattiva della sicurezza