

Titel Endnu mere Firepower med alt det nye frække

Brødtekst

Af IT-afdelingen

Udviklingen og fremskridt stiller større og større krav til vores IT infrastruktur. Særligt anvendelsen af sociale medier og direkte internet kommunikation kræver hurtige og intelligente systemer inden en bruger får klikket på det forkerte billede.

Lige nu er IT afdelingens Infrastruktur & Sikkerhed team i gang med udskifte vores gamle firewalls med den nyeste teknologi.

Årsagen til at de skiftes nu er at få en mere intelligent sikkerhed, større båndbredde på internet forbindelsen og de gamle firewalls var gået ud af service.

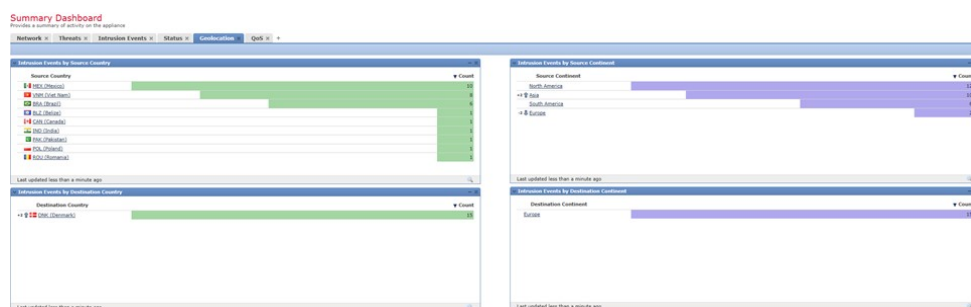


Billede 1. Således ser en Cisco Firepower 2130 ud. Vestforbrænding installerer 2, så der er redundans hvis den ene skulle havarere tager den anden over automatisk.

Al vores trafik til og fra internettet løber gennem vores firewalls, så emails, hjemmeside, KURS, data og lignende skal kontrolleres for vira og tegn på om vi er blevet hacket.

Derfor er disse nye næste generations firewalls, Cisco Firepower 2130, konstrueret med indbygget 6 lags skanning af al trafik samt om der er nogle applikationer som opfører sig mistænksomt.

Blandt de frække ting, set med IT øjne, som de nye firewalls tilbyder er; AVC (Application Visibility and Control), NGIPS (Next Generation Intrusion Prevention System), AMP (Advanced Malware Protection) med videre.



Billede 2. Oversigt over hvor fra vi aktuelt forsøges hacket. Der er ikke nogen russiske sites, da vi har blokeret al adgang til og fra russiske systemer.

Når alt bliver skannet og der bliver alarmeret om unormal adfærd er det med til at der i den seneste version af "Politik for anvendelse af IT" er beskrevet forhold om anvendelse af IT systemer og enheder til private formål, da der så ikke længere kan forventes fortrolighed omkring de data der flyder gennem vores internet forbindelse.

IT afdelingen sidder ikke og læser med når 13% af enhederne i Vestforbrændings netværk har Facebook eller YouTube åbent, for det er en umulig og ganske kedelig opgave. Men der kan være et tegn på en kompromittering som gør at vi omgående skal stoppe og agere på en tråd. Bemærk dog at når de 13% nævnes er det inklusiv mobiltelefoner som er på VestforBYOD netværket.

Da der har været en priskrig på firewalls i USA har vi timet et udbud gennem SKI som har givet os cirka 80% rabat på listeprisen, hvilket gjorde at vi kunne vælge en model med 4.750 Mbits hastighed, hvilket er en ti-dobling af kapaciteten i forhold til de eksisterende. Vi vil på et senere tidspunkt udskifte den gamle SRO firewall med de to som udskiftes, da det vil hæve båndbredden og sikkerheden på forbindelsen til SRO netværket.



Billede 3. Eksempel på en af mange skærbilleder som viser aktivitet baseret på systemer med unormal adfærd. Bemærk hvor meget Facebook og YouTube mandag morgen fylder i trusselsbilledet på Vestforbrænding.

Igennem de næste par uger skifter vi fra de gamle firewalls til de nye. Da vi har fuld redundans i de gamle og nye, forventer vi ikke nogen driftstop – vi vil dog alligevel annoncere servicevinduer på intranettet som sædvanlig.

Udløber	01-01-2100
Afsender	Økonomi & IT
Skrevet	06-09-2019

Oprettet kl. 06-09-2019 10:52 af Julie Kirkegaard (JKI)
 Sidst ændret kl. 06-09-2019 10:52 af Julie Kirkegaard (JKI)

Luk