Reaktiva nät

TOMMY GUSTAFSSON, JONAS ALMROTH,
FREDRIK MÖRNESTEDT

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se

FOI-R--3560--SE
ISSN 1650-1942

December 2012

Tommy Gustafsson, Jonas Almroth, Fredrik Mörnestedt

Reaktiva nät

Bild/Cover: Tommy Gustafsson

Titel	Reaktiva nät
Title	Reactive networks
Rapportnr/Report no	FOI-R--3560--SE
Månad/Month	December/December
Utgivningsår/Year	2012
Antal sidor/Pages	43 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten
FoT område	
Projektnr/Project no	E360221
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informationssystem- och aerosystem

Sammanfattning

Denna rapport beskriver arbetet och resultatet inom projektet ”Reaktiv nätinfrastruktur för dynamisk separation” som genomförts inom ramen för Försvarsmaktens FoT-verksamhet. Projektet har utvärderat och bedömt konceptet reaktivt nät genomförbart. Reaktivt nät är en term som projektgruppen använder för att beskriva ett nätverk som dynamiskt kan anpassa sin säkerhetsnivå baserat på det system eller den typ av information som en viss användare utnyttjar för tillfället. Målet med projektet var att åstadkomma ett nätverk med flera dynamiskt anpassningsbara och logiskt separerade säkerhetsdomäner i en och samma nätinfrastruktur.

Inom projektet har komponenterna till en demonstrator för reaktiva nät utvecklats och värderats. Syftet med demonstratorn är att undersöka huruvida ett reaktivt nät är realiserbart eller ej samt att kunna värdera assuransen för de ingående komponenterna. Vidare kan demonstratorn användas för att visa konceptet med reaktiva nät för beställaren.

Demonstratorn utnyttjar protokollen IEEE 802.1X och SSH för att konfigurera portbaserade accesslistor som åstadkommer den logiska separationen. Projektgruppen har konstaterat att ett reaktivt nät kan byggas baserat på COTS men att den behöver kompletteras med egenutvecklade komponenter. Rapporten fastslår också att reaktiva nät kan fungera som en nätverksbaserad säkerhetsmekanism och att man genom att kombinera tekniken med en MLS-kapabel klient kan underlätta Försvarsmaktens vision om ”en och endast en nät- och informationsinfrastruktur” (FM CIO, 2009).

I rapporten beskrivs också hur reaktiva nät förhåller sig till COTS och de identitetsbaserade nätverk som idag erbjuds från flera tillverkare.

Nyckelord: Reaktiva nät, 802.1X, EAP, identitetsbaserade nätverk, dynamiska accesslistor.

Summary

This report describes the work and result of the Swedish Armed Forces R&T project “Reactive network infrastructure for dynamic separation”. The project have evaluated and assessed a reactive net as feasible. A reactive net is a term used within the project to describe a network that can dynamically adapt its security based on the system or the type of information that a certain user utilizes at every moment. The goal of the project was to achieve and evaluate a network with several dynamically adaptable and logically separated security domains in one single network infrastructure.

Within the project the components of a working demonstrator for a reactive net have been developed and evaluated. The purpose of the demonstrator was to investigate whether or not a reactive net was feasible and to describe the assurance that can be attributed the demonstrator. The demonstrator will also be used to present the reactive net concept to the Swedish Armed Forces.

The demonstrator utilizes the protocols IEEE 802.1X and SSH to configure port-based access lists which provide the logical separation. Such a solution can be based on COTS but needs to be supplemented with some custom components. The report also states that reactive networks can serve as a network-based security mechanism and that by combining such technology with an MLS-capable client, it can facilitate the Swedish Armed Force’s vision of one and only “one network and information infrastructure” (FM CIO, 2009).

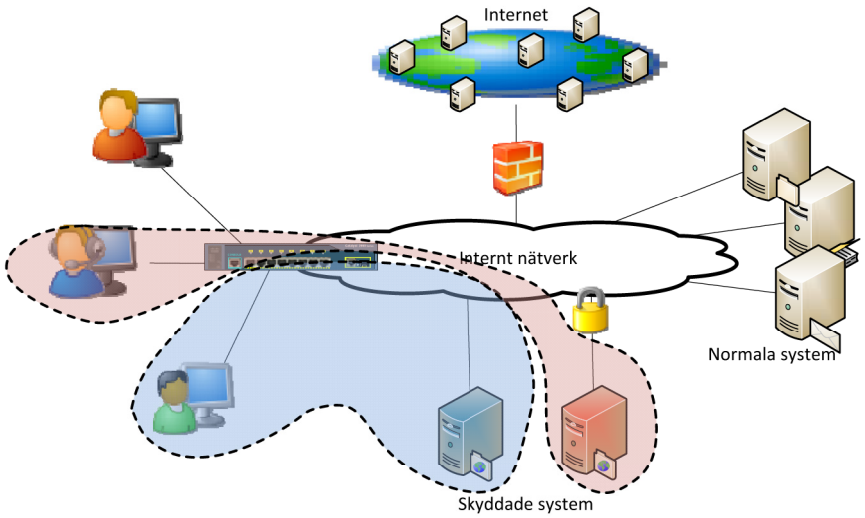
The report also describes how reactive nets are related to COTS and identity-based networks currently offered by several companies as.

Keywords: reactive networks, 802.1X, EAP, identity-based networking, dynamic access lists

Innehållsförteckning

1 Inledning

Ett reaktivt nät är en term som projektgruppen har valt för att beskriva ett nätverk som dynamiskt kan anpassa sin säkerhetsnivå baserat på den känsligheten hos det system eller den typ av information som en användare utnyttjar för tillfället. På så sätt kan nätverket åstadkomma en logisk separation som isolerar användarens klient och som motverkar informationsläckage och intrångsförsök. I Figur 1 visas en gemensam infrastruktur som tillhandahåller nätverksåtkomst till IT-system i flera säkerhetsdomäner.



Figur 1: Översikt av ett målnät för reaktiva nät.

Ordinarie nätverksåtkomst ger användaren tillgång till normala servrar och Internet men när användaren hanterar skyddade system eller uppgifter reagerar nätverket genom att begränsa åtkomsten till omvärlden. Reaktionen sker genom att en så kallad accesslista placeras på användarens port vilket skapar en logiskt separerad säkerhetsdomän. Säkerhetsdomänen kan då begränsas till att endast omfatta användarens klient och det system som användaren behöver. All annan åtkomst förhindras av accesslistan och när användaren återgår till normal användning återställs ordinarie nätverksåtkomst.

Inom projektet har också komponenterna till en demonstrator för reaktiva nät utvecklats och utvärderats. Syftet med demonstratorn var att undersöka huruvida ett reaktivt nät var realiserbart eller ej samt att kunna värdera assuransen för de ingående komponenterna. Vidare kan demonstratorn användas för att visa konceptet med reaktiva nät för beställaren.

Med ett reaktivt nät är det på så sätt möjligt att åstadkomma en dynamisk logisk separation i ett och samma nätverk. Ett fullt utbyggt system med logisk separation för att skydda mot informationsläckage och intrång kräver dock att det reaktiva nätet kombineras med en så kallad MLS-klient. I annat fall riskeras ett läckage genom sårbarheter i klienten.

1.1 Problematisering och frågeställning

Två betydande risker som Försvarsmaktens IT-system måste hantera är risken för informationsläckage och risken för intrång via nätverk. Hotagenterna kan utgöras av allt från främmande makt och APT[1] till enskilda individer och ett aktuellt problem är att hitta en balans mellan dessa risker och behovet av tillgänglighet för behöriga användare. Här kan en plattform baserad på reaktiva nät vara användbar eftersom den kan minska risken för informationsläckage och intrång och samtidigt tillåta en hög informations- och systemtillgång via flexibla säkerhetsmekanismer.

Den totala kostnadsbilden för en IT-miljö påverkas av hur mycket egenutvecklade lösningar i förhållande till kommersiellt tillgänglig teknik, så kallad COTS[2], som används. Grundregeln är att egenutveckling kostar och därför är det attraktivt för Försvarsmakten att i första hand eftersöka lösningar som baseras på kommersiell teknik. Det är dock osäkert vilka säkerhetsnivåer och framförallt assuransnivåer det är möjligt att åstadkomma med kommersiell teknik.

En produktifierad version av reaktiva nät skulle utgöra en säkerhetsmekanism med användning mot informationsläckage och intrång via nätverket. Oavsett hur en säkerhetsmekanism byggs upp eller vilken målsättning den har så är assuransen för en mekanism alltid viktig. Är det inte möjligt att konstatera om en lösning är säker eller ej kan den inte användas som en säkerhetsmekanism. Därför är det viktigt att lyfta in assuransfrågan i utvecklingen så tidigt som möjligt.

För att hantera de problem som lyfts fram ovan skall denna rapport besvara följande frågeställningar:

- Är det möjligt att med COTS åstadkomma en dynamisk nätinfrastruktur som genom logisk separation isolerar en klient baserat på den information och de system som hanteras?
- Vilka faktorer påverkar assuransen för en sådan lösning och vilken assurans kan en sådan lösning tillskrivas?

[1] Advanced Persistent Threat.
[2] COTS, Commercial Off The Shelf.

1.2 Syfte och mål med reaktiva nät

Syftet med denna rapport är att presentera konceptet reaktiva nät och de tekniker som kan användas för att åstadkomma ett sådant. Ett andra syfte med rapporten är att beskriva vilken assurans reaktiva nät kan tillskrivas.

Projektets syfte är att förbättra Försvarsmaktens kunskap inom området och bidrar därmed till utvecklingen mot FM NII med ”en och endast en nät- och informationsinfrastruktur” (FM CIO, 2009).

Målet med ett reaktivt nät är ett effektivare utnyttjande av Försvarsmaktens standardklient genom att samma klient kan användas inom flera säkerhets-domäner. Ett andra mål är att förbättra tillgången till information genom att det blir enklare att konstruera samverkande system. Med en reaktiv nätinfrastruktur på plats kan det vara möjligt att erbjuda en förbättrad tillgång till nätverks-resurser i ett gemensamt nät men med bibehållet skydd mot informationsläckage och intrång via nätverket.

1.3 Avgränsning

Rapporten presenterar endast logiska separationsmekanismer i nätverk och kommer inte att hantera de aspekter som gäller för logisk separation på klienter eller servrar. Rapporten kommer inte heller att analysera de ingående komponenterna på källkodsnivå utan endast på arkitekturnivå.

1.4 Metod

För att besvara rapportens frågeställningar användes följande steg.

1. En proprietär testmiljö för identitetsstyrda nätverk baserade på IEEE 802.1X som hanterar användarautentisering och dynamiska accesslistor konfigurerades. Denna miljö användes som referensmiljö inför steg två.
2. Den proprietära testmiljön överfördes till en öppnare miljö som var lättare att manipulera på ett sätt så att projektets mål kan uppnås. Denna andra testmiljö användes därefter som plattform för demonstratorn som konstruerades i steg tre och fyra.
3. Design av arkitekturen för en demonstrator av reaktiva nät baserad på den kunskap som har inhämtades från steg ett och två. Demonstratorns mål var att åstadkomma en miljö där fokus flyttades från användar-identifiering till system eller informationsidentifiering.

4. Framtagande av demonstratorn baserat på den arkitektur som tagits fram i steg tre. Därefter utvärderas demonstratorns funktion för att se om idén om ett reaktivt nät är realiserbar.
5. För att besvara frågeställningarna om assurans hålls en idékläcknings-diskussion där projektdeltagarna identifierar och värderar de sårbarheter som finns i demonstratorn. Detta är en viktig del för att hantera assuransdiskussionen.

2 Bakgrund

2.1 Ett reaktivt nät

Ett reaktivt nät är en term som projektgruppen har valt att använda för ett nätverk som dynamiskt kan anpassa sin säkerhetsnivå baserat på det system eller den typ av information som en användare utnyttjar för tillfället. Anledningen till att välja en ny term är att detta nätverk skiljer sig från de lösningar som idag finns på marknaden.

Den primära funktionen för ett reaktivt nät är att förhindra informationsläckage genom att neka samtidig nätverksåtkomst till information med olika säkerhetsnivåer. En sekundär funktion för reaktiva nät är att det eliminerar möjligheten att i realtid utnyttja ett system för att studsa ett angrepp och på så sätt angripa ett system på en annan säkerhetsnivå. De lösningar för identitets-baserade nätverk som finns på marknaden idag fokuserar på att begränsa åtkomsten i ett nätverk baserat på argument såsom användaridentitet, anslutande enhet och tidpunkt. Deras primära funktion är därmed att förhindra obehörig åtkomst till ett IT-system.

2.2 Begreppsdefinitioner

Följande förkortningar och begrepp förekommer i rapporten.

Förkortning/ Begrepp	**Betydelse**
802.1X	En standard från IEEE för att använda EAP i trådbunda nätverk.
AD	Active Directory, en katalogtjänst från Microsoft.
Assurans	Innebär att kunna påvisa att det går att hysa tillit/ha förtroende för att det som påstås och att detta verkligen infrias.(FM H SÄK, 2006)
CLI	Command Line Interface, ett textbaserat administrationsgränssnitt, till exempel i en switch.
EAP	Extensible authentication protocol, ett ramverk som används för att initiera en autentisering mellan en klient och en nätverksenhet.
IDM	Identity driven management, en proprietär lösning för identitetsstyrda nätverk från HP.

IBNS	Identity based networking services, en proprietär lösning för identitetsstyrda nätverk från Cisco.
MLS	Multi-Level Security. Ett system som hanterar flera säkerhetsdomäner på en och samma klient.
NPS	Network Policy Server, en RADIUS-server från Microsoft
PCM	ProCurve Manager, en nätverkshanteringsplattform från HP.
PEAP	Protected EAP, en teknik som skyddar EAP med en krypterad tunnel.
RADIUS	Remote Access and Dial In User Service är ett nätverksprotokoll som hanterar autentisering, auktorisering och konfigurationsdata i nätverk.
Reaktivt nät	Ett reaktivt nät är ett nätverk som dynamiskt kan anpassa sin säkerhetsnivå baserat på det system eller den typ av information som en viss användare utnyttjar för tillfället.
SSH	Secure Shell, ett krypterat terminalprotokoll som bland annat används för att hantera nätverksutrustning.

2.3 Autentiseringsprotokoll i nätverk

Autentiseringsprotokoll i ett nätverk har till huvuduppgift att verifiera en enhets eller en användares identitet innan åtkomst till nätverket kan tillåtas. Dessa protokoll har på senare tid även använts för andra uppgifter, såsom att begränsa vilken åtkomst en viss enhet eller användare får eller att godkänna åtkomst baserat på klockslag eller den anslutande enhetens status.

I takt med att antalet funktioner och nätverkstyper som skall stödjas av dessa protokoll har ökat, har även mängden protokoll gjort det. I detta avsnitt ges läsaren en kort orientering för att få ökad kunskap om de protokoll som är relevanta i denna rapport och hur de förhåller sig till varandra.

För autentisering i trådbundna nätverk används följande protokoll:

- EAP, Extensible Authentication Protocol. Ett öppet ramverk som beskriver hur en autentisering skall gå till.

- IEEE 802.1X. En standard som beskriver hur EAP skall implementeras i ett trådbundet nätverk, ibland också refererad som EAP over LAN eller EAPOL.
- PEAP. Ett protokoll som kapslar in EAP i en krypterad tunnel för att åstadkomma en säkrare autentiseringsprocess.

2.3.1 EAP

Extensible authentication protocol (EAP) är ett ramverk som används för att initiera en autentisering mellan en klient och en nätverksenhet, t.ex. en switch eller en accesspunkt. EAP körs direkt ovanpå nivå 2-protokoll såsom Ethernet och PPP och inkluderar egna funktioner för flödeskontroll. Det är ett öppet ramverk som används för att välja en specifik autentiseringsmetod som sedan används för själva autentiseringen (Adoba, B. et al. 2004).

I EAP kallas den anslutande klienten för peer eller supplicant, nätverksenheten för authenticator och mottagande server för authentication server. Mottagande server kan vidareförmedla frågor till en sekundär autentiseringsserver vilket bidrar till det EAPs flexibilitet.

En autentisering sker genom ett fråga-svarförfarande mellan nätverksenheten och den anslutande klienten. Exakt hur det går till beror på vilken autentiserings-metod som används. Först när nätverksenheten är nöjd med autentiseringen kommer den att vidarebefordra paket och ur klientens perspektiv är porten stängd tills dess att autentiseringen slutförts korrekt.

2.3.2 IEEE 802.1X

Hur EAP skall implementeras i trådbundna nätverk beskrivs i IEEE 802.1X. Det är en standard för portbaserad kontroll av nätverksåtkomst som fastslogs 2001 men som har kompletterats 2004 och 2010 (IEEE, 2010). Standarden specificerar hur Extensible Authentication Protocol (EAP) kan utnyttjas för att stödja en centralt administrerad autentiseringsserver och definierar EAP över LAN (EAPOL).

I IEEE 802.1X kallas klienten för supplikant och den implementeras som en mjukvara i klientens operativsystem. I Windows 7 ingår en supplikant som standard och den körs som en tjänst och heter Wired AutoConfig.

2.3.3 Protected EAP, PEAP

EAP erbjuder i sig inget skydd för själva autentiseringsförfarandet och därför har Cisco, Microsoft och RSA Security utvecklat Protected EAP (PEAP). EAP kapslas då in i en TLS-tunnel (Transport Layer Security) som tillhandahåller

kryptering och autentisering under EAP-kommunikationen (Cisco, 2004). När tunneln är etablerad vidtar den normala EAP-autentiseringen som då kan ske på ett mer skyddat sätt.

En autentiseringsmetod som ofta kombineras med PEAP i Windowsmiljöer är Microsofts Challenge Handshake Authentication Protocol (MSCHAPv2). PEAP med EAP-MSCHAPv2 är ett exempel på en EAP-metod där mottagande server använder en sekundär autentiseringsserver. I de testmiljöer som beskrivs i denna rapport används Microsoft Active Directory vilket innebär att autentiseringen kan ske direkt via användarens normala domänkonto.

2.3.4 RADIUS

RADIUS är en förkortning av Remote Access and Dial In User Service och är ett nätverksprotokoll för att hantera autentisering, auktorisering och konfigurationsdata mellan en så kallad Network Access Server (NAS) och en autentiseringsserver (Rigney, C. et al. 2000).

Som namnet antyder var avsikten med RADIUS från början att kontrollera uppringda anslutningar. Tekniken har dock sedan länge används som autentiseringsmetod även i fasta nätverk och används som en defacto-standard för att erbjuda autentisering i samband med IEEE 802.1X. RADIUS-kommunikation skickas i klartext mellan nätverksenheten och servern.

RADIUS erbjuder också möjligheten att skicka tillverkarspecifika attribut, så kallade Vendor-Specific Attributes (VSA) mellan nätverksenhet och server. Dessa kan användas för att konfigurera dynamiska parametrar såsom användarspecifika accesslistor på en switch. Med VSA får varje tillverkare en egen kod, kallad Vendor Code, som identifierar vilken utrustning som skall agera på de bifogade instruktionerna. För att utrustningen skall veta hur den skall tolka instruktionerna föregås dessa av ytterligare en kod som kallas Vendor-Assigned Attribute Number. Hur dessa skall tolkas är upp till respektive tillverkare.

2.4 Accesslistor

Accesslistor är en teknik som i nätverkssammanhang används för att verkställa en åtkomstpolicy i ett nätverk. En accesslista består av en eller flera rader som antingen tillåter eller nekar en viss trafik. Ursprungligen hanterades accesslistor i nätverk av brandväggar men idag används de i både routrar och switchar. Vilka möjligheter en switch har att hantera accesslistor varierar med tillverkare och modell.

Inom de miljöer som beskrivs i denna rapport används två switchar, en Cisco 2960 och en HP 2615. Dessa switchmodeller har ungefär samma förmågor med

avseende på accesslistor och finns i nätverkslagret närmast användaren i många företagsnätverk.

Det finns många olika typer av accesslistor med olika förmågor och de som används i denna rapport är:

- Utökade accesslistor: En teknik som gör det möjligt att sätta regler som avgör åtkomst baserat på avsändaradress, mottagaradress, avsändande port och mottagande port.
- Portbaserade accesslistor: En teknik där en accesslista sätts per port och därmed tillåter olika åtkomstpolicies för olika användare.
- RADIUS-tilldelade accesslistor: En teknik som gör det möjligt för switchen att ta emot accesslistor från en RADIUS-server. Det är i princip en portbaserad accesslista men med skillnaden att den inte konfigureras på själva switchen.

I denna rapport används termen dynamiska accesslistor för att beskriva en accesslista av godtycklig typ som reglerar användarens åtkomst och som anpassas efter gällande säkerhetspolicy.

2.5 Identitetsstyrda nätverk

I dagsläget finns flera lösningar som kan styra åtkomsten till ett nätverk baserat på till exempel identiteten hos den som ansluter, tidpunkten och vilken enhet anslutningen sker med. Dessa nätverk kallas för identitetsstyrda nätverk och styrningen sker vanligtvis genom att med hjälp av RADIUS skicka ut inställningar för accesslistor, prioritet och bandbredd som sätts på den port som användaren ansluter till.

2.5.1 Cisco Identity-Based Networking Services

Identity-Based Networking Services (IBNS) är Ciscos lösning för att tillhandahålla identitetsstyrda nätverk. Lösningen baseras på IEEE 802.1X och utnyttjar RADIUS för att autentisera användaren och tillhandahålla nedladdningsbara accesslistor.

Ciscos lösning är integrerad i Cisco Secure Access Control Server, som bland annat innehåller en egenutvecklad RADIUS-server med integrerad konto-hantering (Cisco 2009). IBNS kan baserat på användaridentitet, tidpunkt, anslutande enhet, anslutningspunkt och enhetens status styra accesslistor, prioritet, bandbredd och VLAN. Hanteringen av användaridentitet kan integreras med Microsoft Active Directory. För att IBNS skall fungera krävs någon form av användarautentisering på switchen, och denna kan till exempel ske via IEEE 802.1X. Systemet kan utnyttja Wired AutoConfig som 802.1X-supplikant.

2.5.2 HP Identity-Driven Management

Identity Driven Management (IDM) är en teknik från HP med målet att öka säkerheten och prestandan i ett nätverk genom att arbeta med dynamiska, användaranpassade policies. Denna styrning sker genom att kontrollera inställningarna på den port som användaren ansluter till vilket innebär att säkerhetsfunktionen kan flyttas till nätverkets gräns. De policies som skall gälla konfigureras via en centralt administrerad server och appliceras på den port som användaren är ansluten till.

IDM är integrerat i HP:s administrationsverktyg ProCurve Manager (PCM) och använder RADIUS för att styra konfigurationen på switcharna. Baserat på användaridentitet, tidpunkt, anslutande enhet, anslutningspunkt och enhetens status kan IDM styra accesslistor, VLAN, prioritet och bandbredd (HP 2006).

IDM kan kombineras med Microsofts katalogtjänst Active Directory och deras RADIUS-server Network Policy Server (NPS). En IDM-agent kompletterar instruktionerna från den ordinarie RADIUS-servern med de policies som sätts via den centrala administrationsservern för IDM. För att systemet skall fungera krävs någon form av användarautentisering på switchen, till exempel via IEEE 802.1X. IDM kan utnyttja Wired AutoConfig som 802.1X-supplikant.

3 Testmiljöer och demonstratorn

För att undersöka hur en lösning baserad på COTS kan hantera dynamiska accesslistor och reaktiva nät utvecklades flera testmiljöer under projektet.

Den första testmiljön baserades på en proprietär COTS-lösning från en av de switchtillverkare som valts ut för demonstratorn. Målsättningen var att bygga upp en referensmiljö med dynamiska accesslistor baserade på användaridentitet. Poängen med att bygga upp en proprietär testmiljö var att en tillverkare säger att det skall fungera och att dokumentation för hur miljön skall byggas finns att tillgå. Baserat på projektgruppens tidigare erfarenhet valdes HP IDM som proprietär lösning.

Med den andra testmiljön var målsättningen att bygga en plattform på vilken demonstratorn kunde konstrueras. Detta skedde genom att eliminera switchtillverkarens proprietära komponenter och därmed få en mer allmän miljö som var enklare att förändra. Även den andra miljön var helt baserad på COTS och här användes en användarkatalog och RADIUS-server från Microsoft. I och med att komponenterna från Microsoft kunde bytas ut mot alternativ från andra tillverkare utan att påverka de dynamiska accesslistornas funktion var denna lösning mindre proprietär än switchtillverkarens. Den andra miljön åstadkoms i viss grad genom att observera RADIUS-trafiken i den första testmiljön med nätverksanalysatorn Wireshark (Wireshark, 2012).

När den andra testmiljön var färdig och dess funktion verifierad påbörjades arbetet med att skapa demonstratorn för reaktiva nät. Målet för denna miljö var att undersöka möjligheterna med att byta ut användaridentiteten mot systemidentitet eller informationsobjekt som styrande variabel för de dynamiska accesslistorna. Demonstratorn baserades i hög grad på den andra testmiljön men kompletterades med egenutvecklade komponenter som hanterade styrningen av användarens åtkomst.

3.1 Dynamiska accesslistor baserade på användaridentitet

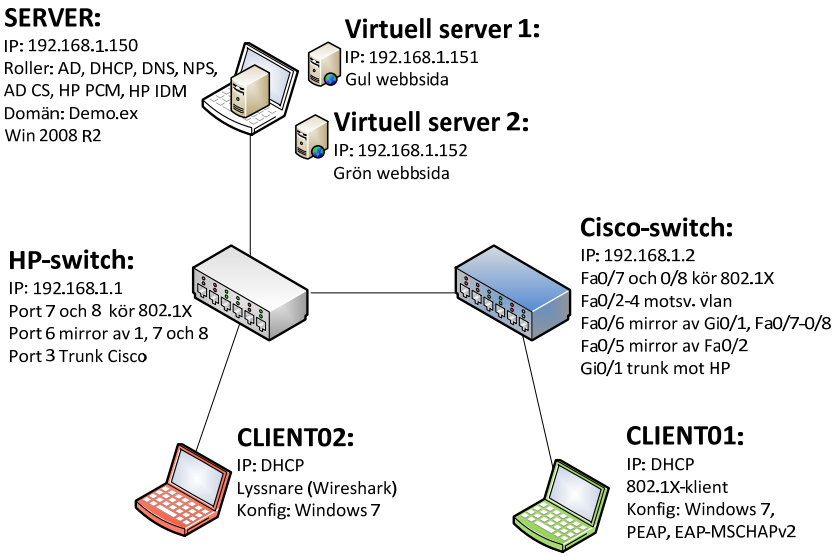
De två första testmiljöerna med dynamiska accesslistor byggdes upp med tre fysiska klienter vars roller och konfiguration fördelades enligt följande:

- SERVER användes som 802.1X-stödjande domänkontrollant med följande konfiguration:
    - Windows 2008 R2 med Active directory, DNS och DHCP
    - Certifikatsserver för att generera ett serversidecertifikat

- RADIUS-servern NPS från Microsoft med PEAP och EAP-MSCHAPv2.

- CLIENT01 simulerade användarens klient och hade följande konfiguration:
  - Windows 7 ansluten till domänen på SERVER
  - Wired AutoConfig med PEAP och EAP-MSCHAPv2
- CLIENT02 användes för att avlyssna och analysera kommunikationen i nätverket och hade följande konfiguration.
  - Windows 7
  - Wireshark nätverksanalysator (Wireshark 2012)

Figur 2 beskriver hur grundkonfigurationen för de två testmiljöerna kopplades ihop med varandra. Switcharna konfigurerades med VLAN, IEEE 802.1X-aktiverade portar och speglade portar för att kunna observera kommunikations-flöden. I början användes RADIUS-kontrollerade VLAN för att snabbt kunna se om klienterna fick instruktioner från RADIUS eller ej. När det konstaterats att VLAN-styrningen via RADIUS fungerade fortsatte arbetet med att skapa de dynamiska accesslistorna.



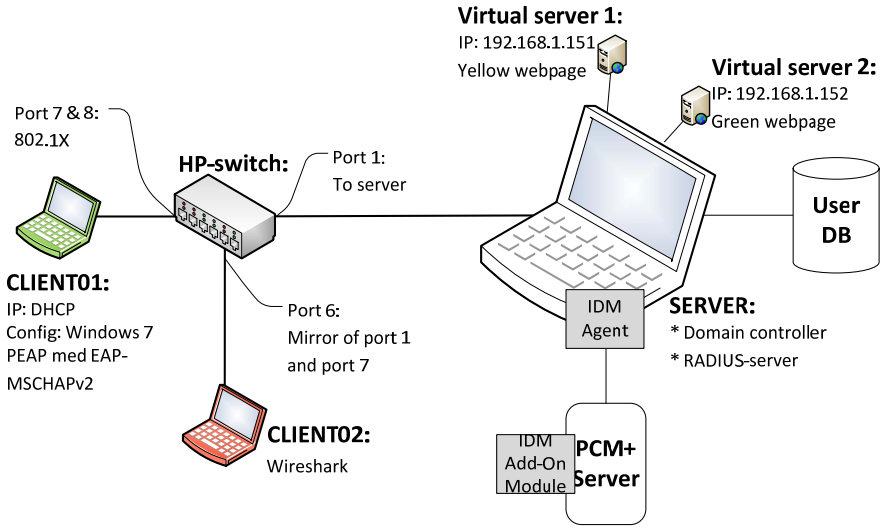
Figur 2: Teknisk uppsättning av testmiljöerna för dynamiska accesslistor.

Den första testmiljön hanterade endast dynamiska accesslistor på HP-switchen men den andra testmiljön hanterar både HP- och Cisco-switchen. Demonstratorns komponenter hanterar inledningsvis endast Cisco-switchen.

För att ha ett par mål att skriva och testa accesslistor mot installerades också två virtuella servrar med varsin webbsida. Dessa servrar placerades på SERVER och utnyttjade samma nätverksanslutning men hade egna IP-adresser.

3.2 Den första testmiljön, HP IDM

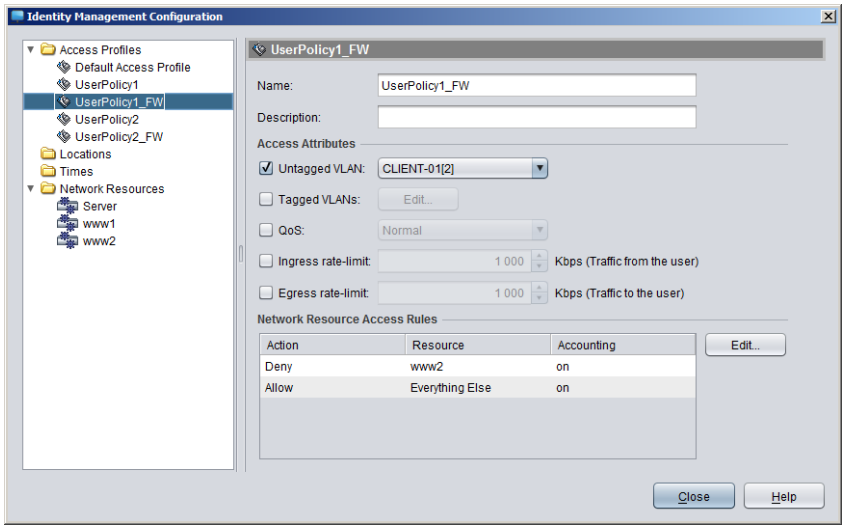
I den proprietära lösningen från HP användes administrationsverktyg PCM+ med tillhörande IDM och IDM-agent. Dessa installerades på SERVER enligt Figur 3 nedan.



Figur 3: Testmiljö för HP Identity Driven Management

I IDM konfigurerades den policy som skall gälla för accesslistan via ett grafiskt gränssnitt. För att kunna konfigurera en policy i IDM skapas så kallade nätverksresurser[3]. Dessa bestod av adress till resursen och inställningar för vilken typ av trafik som skall tillåtas och nekas. I Figur 4 nedan syns SERVER och de två virtuella webbservrarna som nätverksresurser i vänstra menyn.

[3] Eng. Network Resources

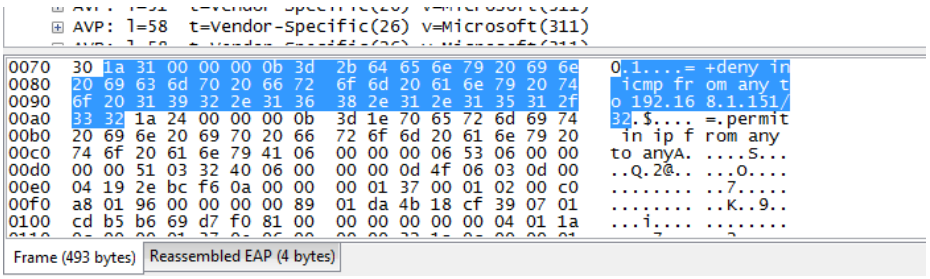


Figur 4: Policygränssnittet i IDM.

När nätverksresurserna skapats användes dessa för att skapa en policy enligt Figur 4 ovan. I detta exempel nekas åtkomst till den virtuella servern www2 men all övrig trafik tillåts.

När policyn var skapad bands denna mot de villkor som skulle gälla för att aktivera policyn. I detta fall användes den grupp som kontot tillhörde på domänkontrollanten för att avgöra vilken policy som skulle gälla.

För att få policyn från den centrala administrationsservern till en accesslista på switchen använder HP sig av RADIUS, i detta fall Microsoft NPS. På RADIUS-servern installeras den så kallade IDM-agenten som tar emot de policies som skapas på IDM-servern och infogar dem i RADIUS-flödet mellan NPS och switchen. (HP 2 2006).



Figur 5: Accesslista skickad från IDM fångad i Wireshark.

I figuren ovan har en rad i accesslistan som skickas till switchen markerats. Av denna kommunikation var det möjligt att utläsa att IDM använde Vendor-Specific Attributes (VSA) och vilken syntax systemet använde för att skicka accesslistorna till switchen.

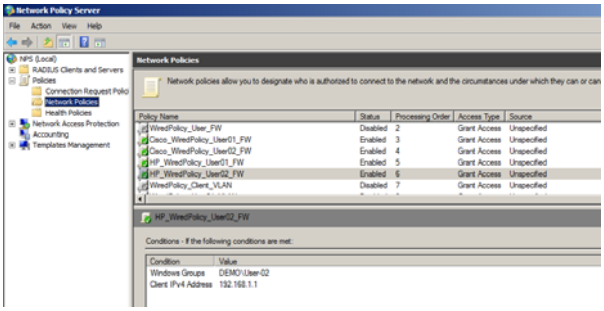
IDM användes endast för att hantera accesslistorna på HP-switchen. Det gick dock inte att finna någon egentlig dokumentation om hur själva policyn skulle konfigureras för att resultera i en viss accesslista på switchen och det visade sig svårt att till exempel få DHCP att fungera.

3.3 Den andra testmiljön, NPS

Den andra testmiljön var en utveckling av den första med målsättningen att överföra IDM:s funktionalitet till Microsofts RADIUS-server för att på så sätt åstadkomma en plattform på vilken demonstratorn kunde konstrueras. Användarens grupptillhörighet utnyttjades för att styra vilken policy som skulle gälla.

HP-switchen och Cisco-switchen hade olika syntax för att konfigurera accesslistor via RADIUS. Kunskapen om hur HP-switchens accesslistor skulle konfigureras i NPS fick inhämtas genom att avlyssna och analysera RADIUS-flödet i den första testmiljön. Kunskapen om hur Cisco-switchens regelverk skulle konfigureras via NPS kunde tillgodoses genom att sammanställa diverse dokumentation från Cisco (Cisco 2, 2004)(Cisco, 2010)(Cisco, 2012).

För att hantera skillnaderna mellan de båda switcharnas sätt att tolka accesslistor används IP-adressen för switchen som en parameter i matchningen av den policy som skulle gälla för en viss inloggning. Totalt krävde en miljö med två användare och två olika switchtillverkare fyra policies enligt Figur 6 nedan.



Figur 6: Policies i NPS-servern.

Samtliga policies i den andra testmiljön hanterade PEAP och EAP-MSCHAPv2. Regelverket för Cisco-switchen konfigurerades genom att utnyttja funktionaliteten att skicka så kallade Cisco-AV-Pair, vilket i princip var VSA

som var namngivna i NPS-gränssnittet. I testmiljön användes en enkel policy som skulle tillåta trafiken till SERVER, DHCP samt HTTP och ping till en av webbservrarna men neka all övrig trafik. Följande syntax användes för att skriva accesslistan som argument i NPS:

```
ip:inacl#1=permit ip any host 192.168.1.150
ip:inacl#2=permit udp any eq bootpc any eq bootps
ip:inacl#3=permit tcp any host 192.168.1.151 eq www
ip:inacl#4=permit icmp any host 192.168.1.151
```

Detta kan jämföras med hur motsvarande regelverk skrivs i switchens textbaserade administrationsgränssnitt, Command Line Interface (CLI)

```
access-list 101 permit ip any host 192.168.1.150
access-list 101 permit udp any eq bootpc any eq bootps
access-list 101 permit tcp any host 192.168.1.151 eq www
access-list 101 permit icmp any host 192.168.1.151
```

Syntaxen för själva regelverket är identiskt men namnsättningen och radnumreringen av accesslistan skiljer mellan CLI och RADIUS.

Motsvarande inställningar gjordes för de båda användarna på en HP- switch. HP kunde inte utnyttja några fördefinerade AV-pair i NPS och fick använda VSA för att konfigurera accesslistorna. I detta fall användes Vendor Code 11 och Vendor assigned attribute number 61 för att ange att det rörde sig om HP respektive en rad i accesslistan. Policyn skulle tillåta all trafik till SERVER, DHCP samt HTTP och ping till en av webbservrarna men neka all annan trafik. Raden för DHCP saknas i accesslistan som sätts via NPS eftersom det inte gick att få till och trots att flera försök med olika formateringar både via IDM och NPS gjordes. Följande syntax användes för att skriva övriga delar av accesslistan som argument i NPS:

```
permit in tcp from any to 192.168.1.150/32
permit in tcp from any to 192.168.1.151/32 80
permit in 1 from any to 192.168.1.151/32
```

Detta kan jämföras med hur motsvarande regelverk skrivs i switchens CLI.

```
ip access-list extended 101
   10 permit ip any host 192.168.1.150
   20 permit udp any eq 68 any eq 67
   30 permit tcp any host 192.168.1.151 eq 80
   40 permit icmp any host 192.168.1.151
```

Som synes är det på en HP-switch en betydande skillnad i hur regelverket anges i switchens CLI och hur det skall skrivas i RADIUS-servern. Det visade sig i de försök som gjordes med DHCP i accesslistan ovan att en HP-switch är väldigt strikt i sin tolkning av den RADIUS-konfigurerade accesslistan. Ett fel i accesslistan leder till att den som helhet ignoreras.

3.4 Verifiering av testmiljöerna

För att kunna verifiera testmiljöns funktionalitet skapades två olika användare som placerades i två olika grupper och som i sin tur bands till två olika policies. Anledningen till att använda grupper på detta sätt är att det blev en mer skalbar lösning där gruppen kunde beskriva en användares roll eller behörighet. De två policierna konfigurerades så att användarna fick olika VLAN och accesslistor och accesslistorna tillät endast åtkomst till en av de virtuella webbservrar som simulerade Internet.

Verifieringen skedde genom att kontrollera användarens åtkomst, dess IP-adress, accesslista och 802.1X-status i switchen samt loggarna från RADIUS-servern. I Figur 7 nedan framgår att en användare på port 7 är autentiserad med hjälp av 802.1X och att denne tilldelats VLAN 2.

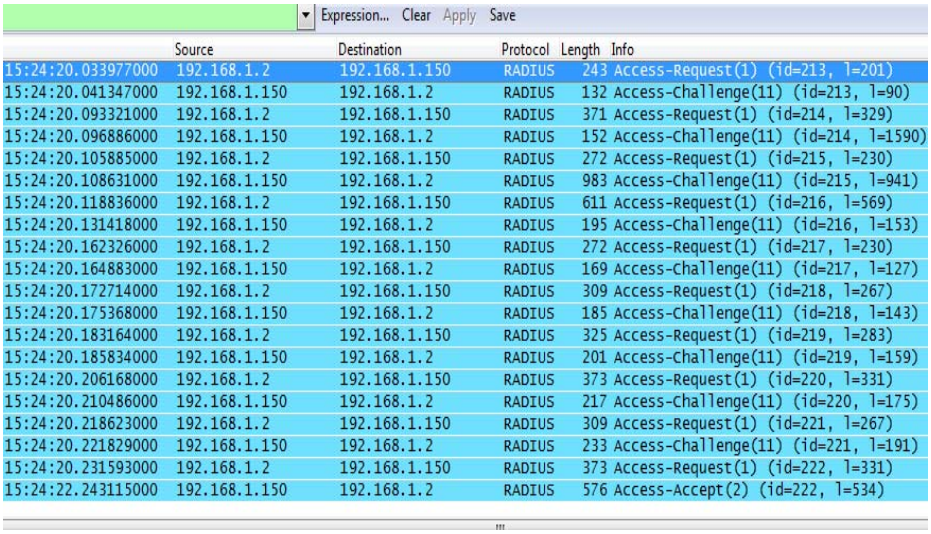
```
Port Access Authenticator Status

 Port-access authenticator activated [No] : Yes
 Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

      Auths/  Unauth  Untagged Tagged          % In  RADIUS Cntrl
 Port Guests  Clients VLAN     VLANs  Port COS  Limit ACL    Dir
 ---- ------- ------- -------- ------ --------- ----- ------ -----
 7    1/0     0       2        No     No        No    No     both
 8    0/0     0       0        No     No        No    No     both


HP-switch#
```

Figur 7: Status för 802.1X på en HP-switch.

3.5 Experiment med klientinloggning

I testmiljöerna med dynamiska accesslistor observerades emellanåt en fördröjning på upp emot en minut mellan användarens inloggning och när den accesslista som konfigurerats i RADIUS hamnade på användarens port. Denna fördröjning kunde påverka säkerheten eftersom ett informationsläckage eller intrång kunde ske till dess att accesslistan var på plats.

Experimentet genomfördes genom att först observera hur den RADIUS-kommunikation som placerade accesslistan på switchen såg ut. Detta flöde kan ses i Figur 8 nedan. Detta jämfördes med statusen för accesslistorna på switchen och då konstaterades att tiden mellan RADIUS-kommunikationen och att accesslistan fanns på användarens port konsekvent var två-tre sekunder.



Expression... Clear Apply Save

	Source	Destination	Protocol	Length	Info
15:24:20.033977000	192.168.1.2	192.168.1.150	RADIUS	243	Access-Request(1) (id=213, l=201)
15:24:20.041347000	192.168.1.150	192.168.1.2	RADIUS	132	Access-Challenge(11) (id=213, l=90)
15:24:20.093321000	192.168.1.2	192.168.1.150	RADIUS	371	Access-Request(1) (id=214, l=329)
15:24:20.096886000	192.168.1.150	192.168.1.2	RADIUS	152	Access-Challenge(11) (id=214, l=1590)
15:24:20.105885000	192.168.1.2	192.168.1.150	RADIUS	272	Access-Request(1) (id=215, l=230)
15:24:20.108631000	192.168.1.150	192.168.1.2	RADIUS	983	Access-Challenge(11) (id=215, l=941)
15:24:20.118836000	192.168.1.2	192.168.1.150	RADIUS	611	Access-Request(1) (id=216, l=569)
15:24:20.131418000	192.168.1.150	192.168.1.2	RADIUS	195	Access-Challenge(11) (id=216, l=153)
15:24:20.162326000	192.168.1.2	192.168.1.150	RADIUS	272	Access-Request(1) (id=217, l=230)
15:24:20.164883000	192.168.1.150	192.168.1.2	RADIUS	169	Access-Challenge(11) (id=217, l=127)
15:24:20.172714000	192.168.1.2	192.168.1.150	RADIUS	309	Access-Request(1) (id=218, l=267)
15:24:20.175368000	192.168.1.150	192.168.1.2	RADIUS	185	Access-Challenge(11) (id=218, l=143)
15:24:20.183164000	192.168.1.2	192.168.1.150	RADIUS	325	Access-Request(1) (id=219, l=283)
15:24:20.185834000	192.168.1.150	192.168.1.2	RADIUS	201	Access-Challenge(11) (id=219, l=159)
15:24:20.206168000	192.168.1.2	192.168.1.150	RADIUS	373	Access-Request(1) (id=220, l=331)
15:24:20.210486000	192.168.1.150	192.168.1.2	RADIUS	217	Access-Challenge(11) (id=220, l=175)
15:24:20.218623000	192.168.1.2	192.168.1.150	RADIUS	309	Access-Request(1) (id=221, l=267)
15:24:20.221829000	192.168.1.150	192.168.1.2	RADIUS	233	Access-Challenge(11) (id=221, l=191)
15:24:20.231593000	192.168.1.2	192.168.1.150	RADIUS	373	Access-Request(1) (id=222, l=331)
15:24:22.243115000	192.168.1.150	192.168.1.2	RADIUS	576	Access-Accept(2) (id=222, l=534)

Figur 8: Ett RADIUS-flöde fångat i Wireshark.

Slutsatsen av denna observation blev då att fördröjningens ursprung antingen berodde på något skeende på servern eller på klienten. Experimentet fortsatte därför genom att studera när det RADIUS-flöde som initierade konfigurationen av accesslisten skickades från klienten i förhållande till när inloggningen gjordes på klienten. Under observationen genomfördes följande försök:

- Uppstart av klienten och inloggning så snart som inloggningsrutan visats.
- Uppstart av klienten och inloggning 30 sekunder efter att inloggningsrutan visats.
- Uppstart av klienten och inloggning 60 sekunder efter att inloggningsrutan visats.
- Växling av användare på en redan uppstartad klient, direkt efter att inloggningsrutan blivit tillgänglig.
- Växling av användare på en redan uppstartad klient, 60 sekunder efter att inloggningsrutan blivit tillgänglig.

I samtliga fall mättes tiden mellan inloggningen och den identifierade RADIUS-kommunikationen med stoppur. Försöken genomfördes både på Cisco-switchen och HP-switchen och mätningarna presenteras i Tabell 1 nedan.

Cisco-switch	Försök 1	Försök 2	Försök 3
Omstart med direkt inloggning	59,0s	57,5s	59,6s
Omstart med 30 s fördröjning	32,2s	32,4s	31,9s
Omstart med 60 s fördröjning	3,4s	3,5s	2,9s
Växla användare, direkt inloggning	50,9s	52,3s	52,3s
Växla användare, 60 s fördröjning	3,1s	2,6s	2,8s

HP-switch	Försök 1	Försök 2	Försök 3
Omstart med direkt inloggning	58,1s	57,9s	58,5s
Omstart med 30 s fördröjning	31,2s	31,8s	31,9s
Omstart med 60 s fördröjning	3,1s	2,8s	2,5s
Växla användare, direkt inloggning	47,3s	46,2s	47,0s
Växla användare, 60 s fördröjning	2,8s	3,2s	2,5s

Tabell 1: Mätvärden från experiment med klientinloggningar.

Resultatet av detta experiment diskuterades inom projektgruppen och slutsatsen blev att RADIUS-kommunikationen påverkades av något på klienten eftersom det är denna som initierar flödet. Projektgruppens teori, som dock inte har kunnat bekräftas, är att fördröjningen beror på när tjänsten Wired AutoConfig startas i Windows.

Experimenten genomfördes på den andra testmiljön men tidigare observationer indikerar att även den första testmiljön påverkas av samma fenomen.

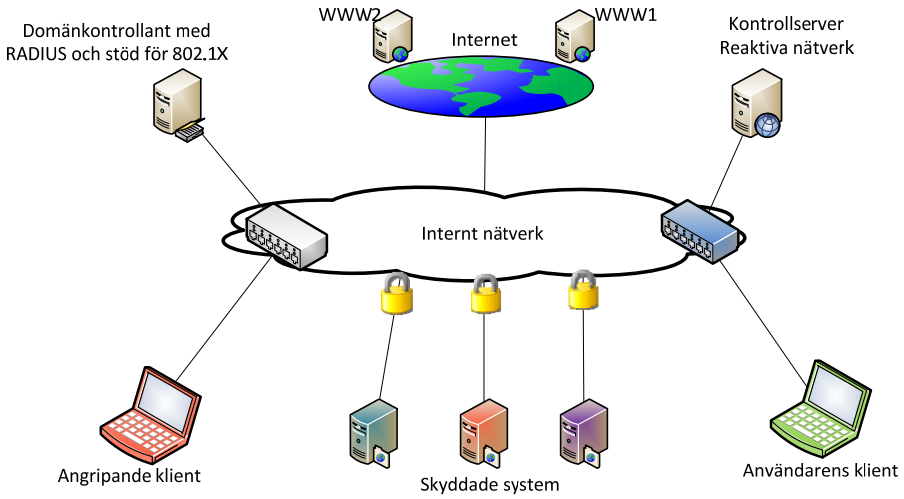
3.6 Utveckling av demonstratorn för reaktiva nät

Syftet med demonstratorn var att undersöka huruvida ett reaktivt nät enligt projektgruppens definition var möjligt eller ej samt vilka komponenter i en sådan lösning som påverkar assuransen. Vidare var tanken att använda demonstratorn för att visa konceptet reaktiva nätverk för Försvarsmakten. För att åstadkomma detta behövde demonstratorn byta ut den utlösningsmekanismen för den dynamiska accesslistan från de två testmiljöernas användaridentitet till ett system eller informationsobjekt.

Demonstratorn skulle därefter använda en dynamisk accesslista för att åstadkomma den logiska separationen som behövs för att kunna hantera flera säkerhetsdomäner på en och samma klient.

Framtagandet av demonstratorn skedde genom att först ta fram en arkitektur och därefter utveckla dess komponenter. Dessa komponenter har utvärderats individuellt och kommer att integreras till en fullt fungerande demonstrator under december 2012.

För att presentera hur ett reaktivt nät kan fungera var demonstratorn uppbyggd som ett mindre företagsnätverk där projektgruppen hade integrerat ett antal komponenter som hanterar dynamiska accesslistor.



Figur 9: Demonstratorns simulerade företagsnätverk

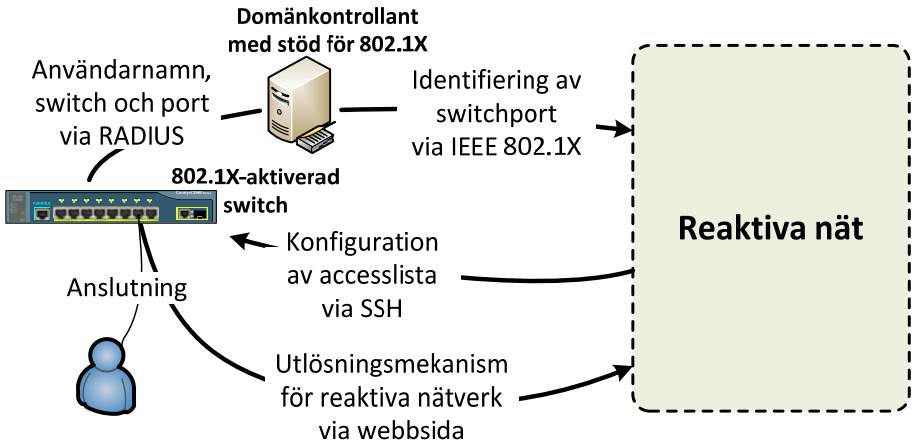
3.6.1 Arkitektur

Vid framtagandet av demonstratorns arkitektur baserades på de kunskaper som insamlats från de två testmiljöerna samt kunskaper om:

- Skadlig kod: Att skadlig kod på klienten kunde påverka utlösnings-mekanismen för reaktiva nät och att skadlig kod kunde anses allmänt förekommande. Andelen datorer som var infekterade med någon form av skadlig kod låg enligt en rapport från Panda Security på drygt 31% perioden under andra kvartalet 2012 (Panda, 2012). Av Försvarsmaktens årsrapport säkerhetstjänst 2011 framgick också att skadlig kod hade utnyttjas vid intrångsförsök mot organisationen (Försvarsmakten 2012).
- Informationsläckage via klienten: Även med ett operativt reaktivt nät kunde ett informationsläckage ske genom att klienten sparade information och skickade den när nätverksåtkomsten återställts.

Arkitekturen måste kunna avgöra var en accesslista skall appliceras, reagera när den skall appliceras och applicera den på den aktuella switchen. För att avgöra

var accesslistan skall applicerade kom projektgruppen överens om att utnyttja användarbaserad inloggning via IEEE 802.1X eftersom användarnamn, switch och port då loggas till RADIUS-servern. För att reagera när accesslistan skall appliceras behövdes en utlösningsmekanism och på grund av problemen med skadlig kod prioriterades en mekanism som kunde användas vid systemåtkomst. Utlösningsmekanismen skulle vara möjlig att byta ut mot till exempel en utlösningsmekanism baserad på filåtkomst i framtida versioner. De problem som påvisades av experimenten med klientinloggningen och det faktum att PEAP-kommunikationen är krypterad gjorde att SSH valdes för att överföra de dynamiska accesslistorna till switchen. Arkitekturen kan ses i Figur 10 nedan.

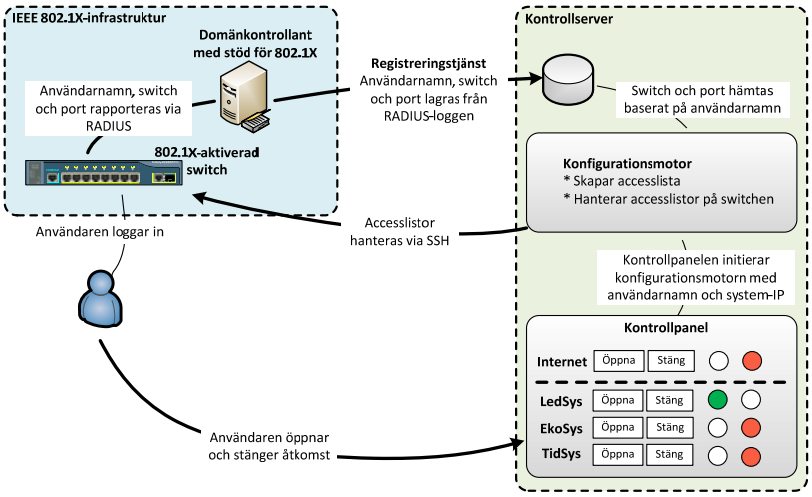


Figur 10: Arkitektur för reaktiva nät med identifiering, utlösningsmekanism och konfiguration.

För att kunna omvandla denna arkitektur till en demonstrator för reaktiva nät fick projektgruppens systemutvecklare anpassa arkitekturen till en systemdesign som sedan kunde kodas. Detta resulterade i fyra huvudkomponenter:

- en 802.1X-aktiverad IT-infrastruktur.
- en registreringstjänst för inloggande användare
- en kontrollpanel som agerade utlösningsmekanism
- en konfigurationsmotor som genomförde inställningarna på switchen

I Figur 11 nedan visas hur demonstratorns komponenter samverkar med varandra.



Figur 11: Samverkande komponenter för demonstratorn av reaktiva nät

IEEE 802.1X-infrastrukturen bestod i demonstratorn av två switchar och en domänkontrollant med stöd för 802.1X. Domänkontrollanten innehöll både kontodatabas och RADIUS-servern som användes för att hantera användarautentiseringen via IEEE 802.1X. Användaren anslöt till en nätverksmiljö som använde 802.1X med PEAP och EAP-MSCHAPv2. Switcharna konfigureras med en accesslista som kallas NORMAL och som sätts som ingående lista på alla användarportar. Denna accesslista har till uppgift att spärra all åtkomst till de skyddade systemen till dess att användaren själv väljer att aktivera denna åtkomst.

Den första versionen av demonstratorn kommer endast att ha möjlighet att hantera accesslistorna Cisco-switchen men projektgruppen bedömer att demonstratorns teknik också kan användas för att hantera switchar från andra tillverkare.

3.6.2 Kontrollserver för reaktiva nät

Kontrollservern var den egenutvecklade del i arkitekturen som gjorde det möjligt att tillhandahålla en nätverksåtkomst som reglerades baserat på de system som användaren ville ha åtkomst till. Den hade till uppgift att:

- underhålla en aktuell databas som kopplade användarnamn till switch och port
- tillhandahålla ett grafiskt gränssnitt från vilket användaren kunde hantera sin åtkomst

- konfigurera rätt port på rätt switch med en accesslista som gav nätverksåtkomst i enlighet med användarens systemanvändning
- tydligt visa statusen för reaktiva nät för användaren

Registreringstjänsten hade till uppgift att initiera en process som hämtade information ur loggfilen från RADIUS och uppdaterade en databas med användarnamn, switch och port när en användare loggade in. Databasen placerades på kontrollservern för reaktiva nät. På så sätt var det möjligt att få en ständigt uppdaterad information om på vilken switch och port en användare befann sig.

När användaren ville ha åtkomst till ett skyddat system gick vederbörande in på en webbsida och valde det aktuella systemet. När en användare klickade på ”öppna” skickades användarnamnet och systemets IP-adress från kontrollpanelen till konfigurationsmotorn. Motorn hämtade användarens switch och port från databasen och skapade en accesslista baserad på typ av switch och vilket system som användaren ville ha åtkomst till. För att reglera åtkomsten loggade konfigurationsmotorn in via SSH in på switchen, skapade den nya accesslistan som namngavs med användarnamnet och bytte ut accesslistan på användarens port. Konfigurationsmotorn bytte accesslistan och verifierade konfigurationen varpå den skickade tillbaka en bekräftelse till kontrollpanelen som då använde de röd/gröna indikatorerna för att visa nätverkets status för användaren.

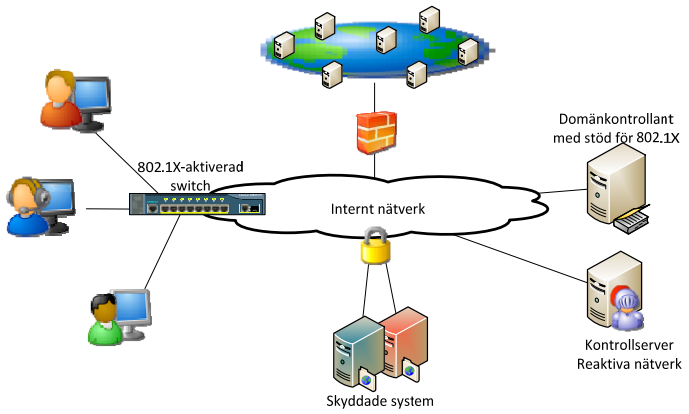
När användaren hade arbetat färdigt med det aktuella systemet gick denne åter in på kontrollpanelens webbsida och klickade ”stäng” för att återställa sin normala åtkomst. Då skickades en ny utlösare till konfigurationsmotorn som via SSH bytte till accesslistan NORMAL på användarens port varpå accesslistan med användarens namn raderades. Efter att ha verifierat konfigurationen skickade konfigurations-motorn tillbaka en bekräftelse till kontrollpanelen som då använde de röd/gröna indikatorerna för att visa nätverkets status för användaren.

3.7 Assuransvärdering

För att värdera assuransen för reaktiva nät genomfördes en idékläcknings-diskussion kring eventuella sårbarheter som fanns i demonstratorns arkitektur och komponenter. Diskussionen utgick från Figur 12 nedan och den funktionsbeskrivande komponentskissen i figur 11 och fokuserade på att identifiera brister i de fyra huvudkomponenter som demonstratorn konstrueras av. De sårbarheter som identifierades värderades baserat på hur sannolika eller komplexa de var att genomföra samt hur stor skada de skulle medföra för säkerhetsmekanismen reaktiva nät.

Assuransvärderingen omfattade också en diskussion om en viss sårbarhet endast förekom i demonstratorkonceptet och hur den i så fall skulle kunna hanteras i en driftsatt version av reaktiva nät.

Assuransvärderingen omfattade inte någon djupare teknisk genomgång av respektive komponent eftersom denna måste göras på de komponenter som används vid ett eventuellt driftsättande av en lösning.



Figur 12: Övergripande arkitektur för reaktiva nät.

3.7.1 802.1X-infrastrukturen

Demonstratorn för reaktiva nät är beroende av att IT-infrastrukturen har stöd för 802.1X och portbaserade accesslistor. De infrastrukturkomponenter som är mest relevanta för att realisera detta stöd är klienten, switchen, katalogservern och RADIUS-servern.

Klienten:

Projektgruppen är överens om att klienten är den enskilt mest sårbara komponenten sett till IT-miljöns helhet men denna hanteras inte inom ramarna för denna rapport. Sett till 802.1X-strukturen så är den enda klientkomponent som är relevant själva supplikanten. Det är tänkbart att manipulera denna på ett flertal sätt för att helt eller delvis slå ut den eller att förfalska de data som den skickar. Detta skulle i princip innebära en DOS-attack mot en enskild klient eller användare.

Switchen:

Switchen är viktig eftersom det är där som policyn verkställs i form av en portbaserad accesslista. Här konstaterades flera potentiella sårbarheter:

- Att manipulera accesslistan NORMAL som förhindrar åtkomst till skyddade system.
- Att manipulera den accesslista som sätts på en port för att tillåta säker åtkomst.

- Att switchen skickar falska svar om statusen för en accesslista.
- Att switchen är korrupt på något sätt och därmed inte fungerar som den ska.
- Att en portbaserad accesslista endast kan filtrera inkommande trafik på en port.

Servern:

I demonstratorns arkitektur hanteras katalogtjänst och RADIUS-server på en och samma fysiska server men det är inte troligt i en driftsatt version av reaktiva nät. Om denna server eller dessa funktioner slås ut åstadkoms en DOS-attack på reaktiva nät och en användare skulle ”fastna” i den accesslista som är aktiv till dess att det reaktiva nätet åter är operativt.

Det är också tänkbart att manipulera inloggningen via 802.1X så att en användare hamnar på fel port och därmed får fel nätverksåtkomst. Denna attack skulle innebära en DOS-attack mot en enskild användare eller port.

3.7.2 Registreringstjänst för inloggande användare

Registreringstjänsten ser till att informationen i den databas som kopplar en användare till en viss switch och port är korrekt. Om denna skulle slås ut skulle innehållet i databasen bli gammalt varpå accesslistorna skulle kunna hamna på fel port. Detta kan tänkas ske genom att antingen attackera tjänsten direkt eller den databas där informationen lagras.

En framgångsrik attack mot registreringstjänsten eller dess stödjande databas skulle innebära att reaktiva nät inte skulle fungera och användarna antingen skulle få fel åtkomst eller ”fastna” i gällande accesslistor.

3.7.3 Kontrollpanelen

Kontrollpanelen innehåller i demonstratorns arkitektur både en utlösare och en statusvy som är kopplade till en webbsida. Genom att angripa denna webbsida är det tänkbart att påverka reaktiva nät och helt eller delvis förse en användare med en felaktig accesslista. Ett angrepp mot webbsidan kan till exempel ske genom sårbarheter i själva webbsidan eller i webbservern. Det är också tänkbart att spoofa sidan och helt enkelt skicka användaren till en förfalskad sida via felaktig ARP eller DNS. Om webbsidan skulle slås ut är det inte längre möjligt för användarna att hantera sina åtkomsträttigheter i nätverket.

En annan variant på angrepp är att manipulera det egna anropet till webbsidan så att man ansluter sig med fel användaridentitet. Detta angrepp skulle troligen resultera i att en accesslista hamnar på fel port eftersom det sker en matchning

mellan användarnamn, switch och port. Detta skulle i princip innebära en DOS-attack mot en eller flera användare.

När det gäller statusvyn så har denna egentligen liten effekt på hur reaktiva nät fungerar eftersom accesslistan inte påverkas av vilken status som signaleras till användaren.

3.7.4 Konfigurationsmotorn

Konfigurationsmotorn ansvarar för att skapa och konfigurera accesslistan på switcharna. Genom att angripa denna komponent är det tänkbart att sätta fel accesslistor eller att helt enkelt ta bort dem från samtliga portar från switchen. I det senare fallet skulle det skydd som reaktiva nät tillhandahåller slås ut.

Dessa sårbarheter måste hanteras genom att säkra konfigurationsmotorn och dess server samt att på sedvanligt sätt begränsa hur SSH-åtkomst kan ske till switchen.

3.7.5 Angrepp i flera steg

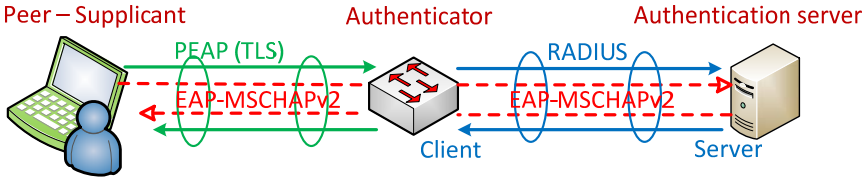
Den arkitektur som projektgruppen valde för att bygga demonstratorn innebar att alla användare delade på en gemensam kontrollserver. Detta är ett val som i sig öppnar för ett angrepp i flera steg. Betänk scenariot att användare A har åtkomst till det skyddade systemet H och kontrollservern K. Användare B har samtidigt åtkomst till Internet och kontrollserver K. Detta innebär att en angripare på Internet kan nå system H genom att gå via användare B, kontrollserver K och användare A. Om kontrollserver K också innehåller konfigureringsmotorn som den gör i demonstratorn så kan en framgångsrik angripare utnyttja detta för att tillförskansa sig kontroll över reaktiva nät.

För att hantera dessa sårbarheter är det viktigt att kontrollservern för reaktiva nät konstrueras på ett sådant sätt att den inte fungerar som en brygga och att den härdas mot angrepp. Det är också en bra strategi att inte husera konfigureringsmotorn på samma server som kontrollpanelen eftersom detta öppnar för angrepp från flera klienter än nödvändigt.

4 Analys och diskussion

4.1.1 Sammanställning protokoll

En autentiserad anslutning till ett trådbundet nätverk åstadkoms genom en kombination av protokoll. Figur 13 nedan visar hur EAP, 802.1X och PEAP kombineras och var man finner respektive komponent. Röd färg används för EAP, blå färg för RADIUS och grön färg för PEAP.



Figur 13: PEAP med EAP-MSCHAPv2 enligt den autentiseringsmetod som används i Reaktiva nät.

Kommunikationen mellan nätverksenheten och klienten är krypterad medan RADIUS-kommunikationen mellan nätverksenheten och servern är okrypterad. Tanken är dock att denna trafik aldrig skall lämna den infrastruktur som man har kontroll över vilket gör det till ett begränsat problem.

4.1.2 Arkitekturen för reaktiva nät

Arkitekturdiskussionen i projektet inleddes med att diskutera hur de fyra komponenter som identifierats som centrala för demonstratorn kunde konstrueras på bästa sätt. Att låta utlösningsmekanismen finnas på användarens klient skulle göra det enklare att både kontrollera filåtkomst och systemåtkomst men samtidigt skulle den vara utsatt för de sårbarheter som finns på klienten och om utlösnings-mekanismen fallerar så fallerar hela plattformen för reaktiva nät. Samtidigt finns det i dagsläget ingen teknik som Försvarsmakten accepterar för att tillåta flera säkerhetsdomäner på en och samma klient varför denna hantering i dagsläget måste ske utanför den egna klienten. Därför valde projektgruppen en lösning med utlösningsmekanismen placerad utanför klienten.

I nästa steg utvärderades möjligheterna med att använda IEEE 802.1X och RADIUS för att konfigurera och verifiera accesslistorna. För att åstadkomma detta måste den teknik som projektgruppen utvecklade initiera ett PEAP-flöde vilket bedömdes för komplext i förhållande till den projekttid som fanns tillgänglig. Dessutom visar försök med 802.1X på Windows 7 att tekniken reagerar för sent för att förhindra ett informationsläckage, med en fördröjning på

uppemot en minut. Därför anser inte projektgruppen att det är en teknik som är användbar för en säkerhetsmekanism mot informationsläckage.

Istället utnyttjas 802.1X endast för att binda en användare till en viss switch och port och SSH för att konfigurera och verifiera de portbaserade accesslistorna. Detta innebär att reaktiva nät utnyttjar en allmänt accepterad teknik för att konfigurera switcharna. Det innebär dessutom att konfigurationen sker krypterat vilket höjer säkerheten i lösningen.

Projektgruppens demonstrator för reaktiva nät består av fyra komponenter:

- en 802.1X-aktiverad IT-infrastruktur med en switch, en domänkontrollant och en RADIUS-server som identifierar den anslutande användaren
- en tjänst på domänkontrollanten som registrerar inloggningar på nätverket och lagrar aktuell switch och port för en viss användare
- en kontrollpanel med en utlösningsmekanism där användaren kan hantera sin åtkomst och som också visar det reaktiva nätets status för användaren
- en konfigurationsmotor som genomför inställningarna på switchen

I versionen som har presenteras i denna rapport används kontrollpanelen också som utlösningsmekanism. Detta innebär i princip att det är systemåtkomsten som styr vilken åtkomst en användare får. Om man istället eftersträvar en lösning där åtkomsten styrs av vilket informationsobjekt som öppnas på användarens klient så behövs en annan utlösningsmekanism. Projektgruppen bedömer att det är fullt möjligt att utveckla en sådan och att den i så fall kan infogas i den nuvarande demonstratorn som ytterligare en utlösningsmekanism. Anledningen att den inte har gjorts är att reaktiva nät i så fall måste kombineras med andra säkerhetsmekanismer för att förhindra informationsläckage som till exempel kan ske genom skadlig kod på klienten.

4.1.3 Logisk separation i nätverket

Den logiska separationen i ett reaktivt nät åstadkoms genom att accesslistor placeras direkt på porten närmast användaren. På så sätt stoppas oönskad trafik så nära källan som möjligt. Hur stark den logiska separationen i nätverket blir är beroende av följande faktorer:

- Accesslistans konfiguration
- Sårbarheter i det reaktiva nätet
- Möjligheten att tunnla trafik via godkända kanaler

En accesslista kan konfigureras mer eller mindre strikt genom att regelverket sätts på nätverkssegment, enskild IP-adress eller protokollens portar. Ju striktare regelverket är, desto bättre blir den logiska separationen.

Sårbarheterna i det reaktiva nätet kan eventuellt användas för att kringgå den policy som skall gälla i nätverket och dessa diskuteras närmare i assuranskapitlet.

Även om det är möjligt att med reaktiva nät stänga av all nätverkstrafik på en viss port under en viss tid så kan denna lösning troligen ses som ett undantag. Med andra ord innebär reaktiva nät att det kommer att finnas godkända kommunikationskanaler och det är fullt tänkbart att dessa kan utnyttjas för att upprätta en så kallad dold kanal[4] via nätverket. Denna risk kan inte helt elimineras men kan minskas med strikta accesslistor och härdning de tjänster som kommunicerar med varandra genom att begränsa den typ av information de kan utbyta. En användare som tillåts kommunicera med flera skyddade system samtidigt ökar också risken för dolda kanaler eftersom det då är möjligt att information från en dator kopieras till en annan dator.

4.1.4 Informationsläckage från reaktiva nät

Reaktiva nät kan endast hantera logisk separation i nätverket och kan inte påverka hur klienten hanterar informationen. Det är till exempel fullt tänkbart att lagra allt som användaren gör och ser i en skyddad session för att därefter vidarebefordra informationen till en obehörig part så fort användarens normala åtkomst återställs. Detta kan antingen ske medvetet av en illvillig användare eller omedvetet till exempel på grund av skadlig kod.

Att användaren medvetet skulle läcka information är ett hot som inte kan hanteras av reaktiva nät och för att lösa detta problem behövs andra säkerhetsmekanismer som inte hanteras vidare i denna rapport.

Skydd mot omedvetna informationsläckage genom principen att lagra information för att läcka senare kan hanteras genom att reaktiva nät kombineras med annan teknik. Ett exempel vore att kombinera reaktiva nät och krypterade lagringskapslar[5], ett koncept för att konstruera ett MLS-system med hjälp av virtualisering och filkryptering som har tagits fram av en forskargrupp vid University of Michigan (K. Border et al. 2009).

I konceptet används två virtuella klienter som körs på en minimalistisk hypervisor. Användaren utför det mesta av sitt arbete på den primära klienten som innehåller ett normalt operativsystem och alla applikationer som användaren

4 Med dold kanal menas i denna rapport en väg där information kan läcka utan att användaren avser och/eller känner till det.

5 Eng. Storage capsules

behöver. Den säkra klienten innehåller endast ett minimalt operativsystem vars uppgift är att hantera de krypterade enheter som skyddar informationen när den inte används.

När en användare vill arbeta med känslig data tas en avbildning[6] av den primära klienten varpå all kommunikation till utgående nätverk stängs av. Därefter dekrypteras den kapsel som användaren vill använda och denne kan nu arbeta med sina känsliga data med hjälp av de applikationer som finns på den primära klienten. När användaren vill återgå till det normala läget krypteras kapseln, den primära klienten återställs från avbildningen vilket innebär att alla eventuella förändringar som gjorts raderas och det utgående nätverket aktiveras igen.

En svaghet med konceptet är att det är ett system som inte tillåter någon nätverkskommunikation alls i det säkra läget. Men genom att kombinera tekniken med reaktiva nät skulle det vara fullt möjligt att erhålla det klientbaserade skyddet mot informationsläckage samtidigt som man tillät en kommunikation till utvalda system.

4.2 Möjligheter med COTS

Under projektet har HP:s plattform för identitetsstyrda nätverk, IDM, testats. Detta är en proprietär lösning som via 802.1X kan hantera åtkomst till nätverket baserat på användaridentitet, anslutande system, tidpunkt med mera. En studie av dokumentationen visar att Ciscos proprietära lösning IBNS har motsvarande funktionalitet. Ingen av dessa lösningar har möjlighet att hantera accesslistor baserad på vilken information som en användare öppnar eller vilket system denne arbetar med. Troligen beror detta på att dessa lösningar har som mål att skydda nätverket från obehörig åtkomst förr än att förhindra informationsläckage.

Projektgruppen har också lyckats med att överföra de proprietära systemens funktionalitet till en lösning som baseras på katalogtjänst och RADIUS-server från Microsoft. Det är också möjligt att överföra denna lösning till andra katalogservrar och RADIUS-servrar. Inte heller dessa lösningar har möjligheten att hantera åtkomst baserat på informationsobjekt eller systemåtkomst.

I projektet har switchar från två leverantörer används för att utvärdera hur olika tillverkare hanterar dynamiska och portbaserade accesslistor, en Cisco 2960-8TT-L och en HP 2615-8-PoE. Projektgruppens försök med switcharna har påvisat vissa skillnader i hur de kan hantera dynamiska accesslistor via RADIUS, och det har inte gått att konstruera ett relevant nätverk på switchen från HP. Detta påverkar inte den föreslagna lösningen för reaktiva nät eftersom accesslistorna då hanteras via SSH istället för RADIUS.

[6] Eng. Snapshot

De försök som har gjorts med Windows 7 och 802.1X visar att 802.1X som säkerhetsmekanism har en betydande svaghet eftersom det kan dröja upp emot en minut innan ett regelverk finns på plats på porten. Detta verkar bero på när i operativsystemets startsekvens Microsoft har valt att starta tjänsten Wired Autoconfig. Eventuellt kan denna svaghet dock hanteras genom att byta till en 802.1X-supplikant som startar tidigare. I och med att accesslistorna i demonstratorn hanteras via SSH påverkar fördröjningen inte säkerhetsnivån i reaktiva nät.

Sammantaget visar projektgruppens arbete att det inte är möjligt att bygga en lösning med reaktiva nät som enbart baseras på COTS eftersom det inte finns några lösningar som utnyttjar accesslistor i nätverket för att förhindra informationsläckage. Valideringen av demonstratorns komponenter som presenteras i rapporten visar dock att det genom att komplettera COTS med en begränsad mängd egenutvecklade komponenter är möjligt att åstadkomma reaktiva nät.

4.3 Assurans

Hög assurans för en lösning som bygger på logisk separation är så svår att fastställa att Försvarsmakten hittills inte anser att logisk separation kan användas som en säkerhetsmekanism. Som tidigare fastslagits hanterar reaktiva nät endast säkerheten i nätverket och bör därför kombinerads med en MLS-klient för att skydda bättre mot intrång och informationsläckage.

Assuransdiskussionen för reaktiva nät kommer att ske på tre olika nivåer. På övergripande nivå är det intressant att utreda hur informationen kan skyddas med hjälp av tekniken. På arkitekturnivå är det lösningens teknikval, de komponentstrukturer och de eventuella sårbarheter som dessa medför som diskuteras. Därunder finns också en mer teknisk nivå som hanterar hur lösningens komponenter produceras. Den tekniska assuransdiskussionen är hårt knuten till vilka teknikval som görs i en eventuell lösning för reaktiva nät och kommer därför inte att hanteras i denna rapport.

4.3.1 Assurans på övergripande nivå

På den högsta nivån handlar assuransen om tilltron till att reaktiva nät kan fungerar för att öka Försvarsmaktens skydd mot informationsläckage och intrång. Även om reaktiva nät fungerar på det sätt som projektgruppen förväntat sig är det inte en säkerhetsmekanism som kan användas för att skydda sekretessklassade uppgifter i högre informationssäkerhetsklasser. Det kan dock vara intressant att vidare utreda hur reaktiva nät kan användas för att hantera mindre känsliga uppgifter och eventuellt stödja Försvarsmaktens strävan mot en gemensam IT-infrastruktur.

Här kan projektgruppen konstatera att en lösning med reaktiva nät kan tillföra ett skydd mot informationsläckage och intrång i en klientmiljö som överspänner flera säkerhetsdomäner. Det är också en tänkbar lösning som kan användas för att begränsa åtkomst och höja den övergripande säkerhetsnivån inom en och samma säkerhetsdomän.

För att reaktiva nät skall stödja Försvarsmaktens strävan att nå flera system från en och samma klient måste dock reaktiva nät kombineras med tekniker som åstadkommer logisk isolering på klienten.

4.3.2 Assurans på arkitekturnivån

Under den idékläckningsdiskussion som projektgruppen genomförde framkom flera sårbarheter. De möjliga konsekvenserna av dessa sårbarheter kan i princip kategoriseras sådana som har DOS-relaterade och sådana som har funktions-relaterade konsekvenser. Den senare kategorin är den allvarligare av de två eftersom denna kan medföra att det skydd som reaktiva nät medför helt eller delvis slås ut.

De angrepp som kan leda till funktionsrelaterade konsekvenser bedömer dock projektgruppen som relativt komplexa att genomföra eftersom de kräver att en angripare kan åstadkomma förändringar i framförallt switchens konfiguration. En produktionslösning för reaktiva nät måste designas med ett särskilt fokus på dessa sårbarheter. En metod för att begränsa denna sårbarhet vore att endast tillåta SSH-kommunikation på en port och via ett nät som i övrigt inte är nåbart.

Ett annat angrepp som eventuellt kan påverka klienten är det faktum att en portbaserad accesslista endast filtrerar inkommande trafik på en viss port. Därmed finns en möjlighet att en angripare kan skicka instruktioner till klienten i blindo, till exempel via UDP eller blind TCP. Ett sådant angrepp måste dock ske från en position i nätverket med vissa privilegier och dessutom vid rätt tidpunkt för att lyckas och även vid en lyckad attack är det svårt att påverka användarens klient på ett effektivt sätt. Projektgruppens bedömning är därför att denna typ av angrepp är så komplicerad att genomföra och kräver så mycket tur (för att kunna genomföra det vid rätt tidpunkt) att denna risk kan anses försumbar.

Angrepp som kan leda till DOS-relaterade konsekvenser är flera och bedöms enklare att genomföra. Det kan till exempel handla om attacker mot den stödjande infrastrukturen, en enskild klient eller mot kontrollservern. Genom att designa en produktionslösning med dessa sårbarheter i åtanke kan de allra flesta risker minimeras. Ett DOS-relaterat angrepp skulle endast leda till begränsad tillgänglighet för användaren och skulle inte leda till något informationsläckage.

5 Slutsatser

Nedan presenteras projektgruppens slutsatser.

5.1 Slutsatser kopplade till frågeställningarna

5.1.1 Lösningens genomförbarhet

Projektet visar att de komponenter som ingår i demonstratorn fungerar och att det är möjligt att konstruera ett reaktivt nät enligt projektgruppens definition. Tekniken för att åstadkomma ett reaktivt nät finns tillgänglig men den kräver en anpassning utöver COTS. De COTS-lösningar som finns på marknaden i dagsläget fokuserar på att skydda nätverket från obehörig åtkomst men har svårt att hantera informationsläckage. Därför är en lösning med reaktiva nät inte genomförbar med endast COTS men demonstratorn visar att den är möjlig att åstadkomma genom att kombinera COTS med begränsad egenutveckling.

5.1.2 Assurans

När det gäller assurans är den stora utmaningen att åstadkomma en tillräcklig assurans för en lösning som baseras på logisk separation. Projektgruppens assuransdiskussioner kring demonstratorns arkitektur och komponenter visar att det finns sårbarheter som behöver utredas vidare. Men projektgruppen har heller inte funnit någon enskild sårbarhet som innebär att reaktiva nät är helt uteslutna ur assuranssynvinkel.

De angrepp som skulle få de allvarligaste konsekvenserna bedömer projektgruppen vara om en angripare lyckas manipulera switchens accesslistor, antingen direkt eller via konfigurationsmotorn. De minst komplexa, och därmed mest sannolika angreppen kan dock riktas mot lösningens tillgänglighet och här finns det flera möjliga angreppsalternativ.

5.2 Övriga slutsatser

5.2.1 Kombinera reaktiva nät med MLS-klienter

Även om reaktiva nät i sig skulle kunna ge ett visst skydd för känsliga system så är det först när tekniken kan kombineras med en MLS-klient som den blir riktigt intressant. Projektgruppens arbete visar att ett reaktivt nät då gör det möjligt att omvandla en isolerad lösning till en lösning som både kan skydda information och kommunicera med andra system. Detta gör tekniken intressant att undersöka

vidare för att se om den kan användas för att uppfylla Försvarsmaktens vision om en och endast en nät- och informationsinfrastruktur.

5.2.2 RADIUS-hantering av dynamiska accesslistor

Projektgruppens observationer visar att det finns en viss fördröjning kopplad till RADIUS-hanterade accesslistor. Denna fördröjning måste hanteras för att tekniken skall utgöra en realistisk säkerhetsmekanism. I och med att demonstratorns konfigurationsmotor istället utnyttjar SSH så undviks detta problem i reaktiva nät.

5.2.3 Identitetsstyrda nätverk via Microsoft NPS

Flera switchtillverkare tillhandahåller idag egna lösningar för identitetsbaserade närverk men projektet visar att det är fullt möjligt att utnyttja öppnare lösningar för att åstadkomma denna funktion.

6 Fortsatt arbete

Under projektet har ett antal frågeställningar identifierats som det inte har funnits möjlighet att hantera inom projektet.

6.1 Accesslistor i en switch

Hur hög säkerhet kan man anse att en accesslista i en switch kan åstadkomma i förhållande till de accesslistor som sitter i en brandvägg? För att besvara denna fråga vore en lämplig metod att studera sårbarheter för switch respektive brandväggar och analysera hur dessa kan utnyttjas i relation till reaktiva nät. Metoden bör också undersöka hur en switch jobbar med sin filtrering och vilka tekniker som switchen kan utnyttja.

6.2 Kombination av reaktiva nät och MLS

Som tidigare konstaterats hanterar reaktiva nät endast vissa delar av de sårbarheter som kan leda till informationsläckage. Det vore därför intressant att utreda möjligheterna att kombinera reaktiva nät med klientbaserade virtualiseringstekniker för att åstadkomma MLS och för att se om kombinationen kan användas för att uppfylla Försvarsmaktens vision om en och endast en nät- och informationsinfrastruktur. I samband med en sådan studie vore det också intressant att undersöka hur en filstyrd utlösningsmekanism skulle kunna kontrolleras.

6.3 Införande av reaktiva nät

Den lösning som presenterades i denna rapport bedömer projektgruppen så pass realiserbar att det vore intressant att undersöka hur ett faktiskt införande skulle kunna gå till och hur det skulle påverka den övergripande säkerhetsnivån i nätverket. En annan intressant fråga som behöver hanteras är till exempel vad som händer när en användare inte loggar ut eller återställer sin åtkomst.

7 Referenser

FM CIO (2009). CIO Måldokument för Nät- och Informationsinfrastruktur (NII), Försvarsmakten, Bilaga till 09 100.64095, 2009-09-24

FM H SÄK (2006). Handbok för Försvarsmaktens säkerhetstjänst, Informationsteknik, H Säk IT 2006. Försvarsmakten, 10 440:66817

Adoba, B. et al. (2004). Extensible Authentication Protocol (EAP), Internet Engineering Task Force, RFC 3748

IEEE (2010). IEEE Standard for Local and metropolitan area networks – Port-based Network Access Control. IEEE Computer Society

Cisco (2004). Protected EAP (PEAP) Application Note, Cisco Systems Inc. OL-6005-01

Rigney, C. et al. (2000). Remote Authentication Dial In User Service (RADIUS). Internet Engineering Task Force, RFC 2865

Cisco (2009). Identity-Based Networking Services (IBNS), Cisco Systems Inc, C45-504537-01 07/09

HP (2006). Delivering Intelligent Network Access Through Identity Driven Management, IDM Whitepaper. Hewlett-Packard Development Company, 4AA0-2000ENW Rev. 1, 3/2006

www.wireshark.org. Wireshark – Go Deep. 2012-11-20

HP 2(2006). Identity Driven Management - Technical Brief. Hewlett-Packard Development Company, 4AA0-0106ENW Rev. 1, 3/2006

Cisco 2 (2004), Sample Configuration Guide for Cisco Secure ACS and PIX Firewall – Chapter 3 - ACLs with RADIUS. Cisco Systems Inc, OL-5644-01.

Cisco (2010), Catalyst 2960 Desktop Switch Software Configuration Guide – Chapter 31 - Configuring Network Security with ACLs. Cisco Systems Inc, OL-8603-09.

Cisco (2012), IEEE 802.1X with ACL Assignments. Cisco Systems Inc.

Panda (2012), Quarterly Report PandaLabs April-June 2012. Panda Security

Borders, K.; Weele, E. V.; Lau, B. & Prakash, A. (2009), Protecting Confidential Data on Personal Computers with Storage Capsules., in 'USENIX Security Symposium' , USENIX Association, , pp. 367-382 .