HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

NAC i NAP sustavi

CCERT-PUBDOC-2007-06-194

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

NAC (eng. *Network Admission Control*) i NAP (eng. *Network Access Protection*) su dva nezavisno razvijena sustava za povećanje sigurnosti lokalnih korporativnih mreža. NAC sustav razvila je tvrtka CISCO dok je NAP razvio Microsoft, a zajednička im je težnja ka povećanju sigurnosti lokalnih mreža utemeljena na osiguravanju provođenja sigurnosnih politika u svim dijelovima mreže, tj. na svim računalima koja mrežu koriste. I jedan i drugi sustav koriste vlastite protokole za provjeru sigurnosnih parametara pojedinog računala, te mu na osnovu utvrđenog stanja u određenoj mjeri ograničavaju ili dozvoljavaju pristup mrežnim resursima. Isto tako oba sustava omogućuju automatiziranu provedbu usklađivanja računala s definiranom sigurnosnom politikom. Cilj im je jednak – smanjiti rizik kompromitiranja mrežne sigurnosti zbog nemarnih korisnika koji ne provode sigurnosnu politiku nad svojim računalima ili pak zbog korisnika koji mrežu koriste samo povremeno pa nisu u mogućnosti pratiti propisana sigurnosna pravila.
U ostatku dokumenta općenito je opisan problem računalne sigurnosti te je detaljno analizirano na koji ju način i uz koje zahtjeve osiguravaju dva spomenuta sustava.

2. Općenito o računalnoj sigurnosti

Računalna sigurnost može se načelno podijeliti u tri područja:

- Operativna sigurnost koju čine:
  - sigurnosna politika,
  - edukacija,
  - detekcija uljeza,
  - praćenje razine mrežnog prometa,
  - proaktivna provjera ranjivosti,
  - *honeypot* sustavi te
  - sigurnosne vježbe.
- Sigurnost aplikacija i računala koju čine:
  - sigurnosne zakrpe i konfiguracija,
  - pravilna autentikacija,
  - filtriranje mrežnih paketa na razini računala,
  - enkripcija sjednica uz korištenje sigurnih aplikacijskih protokola,
  - naslijeđeni sustavi i neosigurane usluge,
  - odvajanje usluga te
  - konfiguracija osobnih računala.
- Mrežna sigurnost koju čine:
  - izolacija putova i VPN (eng. *Virtual Private Network*) i
  - zaštita zone.

O svakom od ovih područja bit će riječi u sljedećim poglavljima.

2.1. Operativna sigurnost

Operativna sigurnost ili proceduralna zaštita je vrlo široko područje iz kojeg treba istaknuti nekoliko ključnih elemenata.

Sigurnosna politika – definira tko može ili ne može činiti nešto. Definiranje sigurnosne politike uključuje identifikaciju sigurnosnih prijetnji te određivanje njihovih prioriteta kao i identifikaciju sigurnosnih pretpostavki (npr. područja zaštite, provjereni sustavi i infrastruktura). Tek kad je politika definirana i uspostavljena potrebno ju je podržati odgovarajućim standardima te prikladnim resursima i alatima za administraciju računala, tj. tek kad se definiraju zahtjevi na sigurnost može se projektirati zaštita.

Edukacija o sigurnim/nesigurnim načinima korištenja računala. Sigurnost je odgovornost svih korisnika pa ih je sve nužno u odgovarajućoj mjeri učiniti svjesnima problema.

Detekcija uljeza – sastoji se od upotrebe alata koji detektiraju uzorke unutar mrežnog prometa i tako raspoznaju uljeza. Mišljenja o korisnosti detekcije uljeza su podijeljena. Uz porast mrežnih kapaciteta i prometa malo je vjerojatno da se detekcijom alarmantnih uzoraka u prometu može osigurati kvalitetna zaštita. Ona međutim može biti korisna ako se primjenjuje na razini određenih poslužitelja ili može poslužiti za ocjenu ispravnosti vatrozidnih pravila. S druge strane sofisticirani napadači će vjerojatno napad izvršiti na klijentsko računalo, a ne direktno na poslužitelj što će sustav za detekciju uljeza zabilježiti kao pristup normalnog korisnika poslužitelju i neće generirati alarm.

Praćenje razine mrežnog prometa – metoda zaštite koja se temelji na detekciji porasta mrežnog prometa iznad određene razine. Ova metoda je nešto pouzdanija od detekcije uljeza, ali uz nju mora biti omogućeno ispitivanje specifičnih tokova prometa u situacijama kad se povećanje prometa stvarno detektira.

Proaktivna provjera ranjivosti – sastoji se od upotrebe alata kojima se periodički provjerava sigurnost mreže. Može se raditi centralno za cijelu mrežu ili po dijelovima mreže, ali da bi dala rezultate mora se provoditi periodički i redovito.

***Honeypot* sustavi** ili mamci za napadače su u osnovi sustavi koji su namjerno oslabljeni kako bi privukli napadače s ciljem identifikacije ili odvlačenja njihove pažnje od kritičnih sustava.

Sigurnosne vježbe – sastoje se od povremenih simulacija DoS (eng. *Denial of Service*) napada, ubacivanja virusa ili oštećenja podataka sa svrhom provjere i popravljanja sigurnosnih mjera zaštite.

Preporuka je takve provjere raditi u razdobljima kad mreža i poslovanje organizacije nisu pod velikim opterećenjem.

2.2. Sigurnost aplikacija i računala

Sigurnost aplikacija i računala postiže se njihovom pravilnom konfiguracijom. Kako bi se ona uspostavila potrebno je voditi računa o parametrima opisanim u daljnjem tekstu.

Sigurnosne zakrpe i konfiguracija – istraživanja pokazuju da se većina uspješnih napada na računalne sustave temelji na iskorištavanju malog broja sigurnosnih propusta u operativnim sustavima ili aplikacijama, ali također pokazuju i da se većina tih napada može spriječiti instalacijom sigurnosnih zakrpi.

Kada se govori o određivanju pravilne konfiguracije potrebno je uočiti razliku između konfiguracije klijenta i poslužitelja. Konfiguracija klijenta je znatno teža jer je na njemu uobičajeno potrebno omogućiti korištenje e-mail klijenta i web preglednika koji udaljenom napadaču omogućuju kompromitiranje sustava iskorištavanjem postojećih sigurnosnih propusta i navođenjem korisnika na odgovarajući oblik suradnje . Jednom kada je klijent probijen, napadač može lako doći i do poslužitelja.

Pravilna konfiguracija klijenata trebala bi uključivati kompleksne tajne ključeve pohranjene na npr. *smart* kartici i korištenje dvosmjerne ili tzv. *challenge – response* autentikacije kako bi se smanjila mogućnost proboja bez znanja korisnika. Kod poslužitelja je situacija nešto drukčija pa se tako preporuča isključivanje svih nepotrebnih poslužiteljskih usluga i ograničenje pristupa poslužitelju samo preko određenih priključaka. Također, trebalo bi izbjegavati slanje informacija nezaštićenim protokolima.

Pravilna autentikacija – jedan od najvećih sigurnosnih rizika predstavlja slanje autentikacijskih podataka s klijenta na poslužitelj nezaštićenim kanalom. Zato je prvi korak pravilne autentikacije osiguravanje zaštićene i sigurne razmjene autentikacijskih podataka. Za zaštitu se mogu koristiti dvije tehnike: zaštita aplikacijskim/pristupnim protokolom (npr. SSH, SSL, Kerberos) ili zaštita sigurnim transportnim protokolom (VPN). Budući da se kompromitiranjem klijenta može doći do statičkih korisničkih autentikacijskih podataka (korisničkog imena i zaporke), preporuča se korištenje tajnih ključeva (*smart* kartica) i dvosmjerne autentikacije za pristup osjetljivim poslužiteljima. Jedna od mogućih sigurnosnih postavki je i uspostava dodatne autentikacije za modifikaciju podataka koja djeluje nezavisno od autentikacije za čitanje podataka.

Filtriranje paketa na razini računala – postiže se implementacijom neke vrste vatrozida na samom računalu, čime se podiže ukupna razina sigurnosti. Primjer takve zaštite je filtriranje paketa na osnovu TCP omotnice paketa ili na osnovu IP tablica čime se, primjerice, omogućava zaustavljanje svih paketa pristiglih izvan lokalne domene. Ova metoda zaštite ide u smjeru pomicanja granica zaštite prema rubovima zaštićene zone, tj. rubovima mreže i posebno je efikasna u sprečavanju korisničke uporabe manje sigurnih protokola. Filtriranje na osnovu IP tablica također pomaže i u sprečavanju napada prepisivanjem spremnika jer filtri zlonamjerno oblikovane pakete zaustavljaju prije nego stignu do transportnog OSI sloja, tj. prije nego postanu opasni.

Enkripcija sjednica sigurnim aplikacijskim protokolima jedan je od najboljih načina zaštite prijenosa osjetljivih podataka. Pritom se prvenstveno misli na tri protokola: SSL (eng. *Secure Socket Layer*) za web aplikacije te SSH (eng. *Secure Shell*) i Kerberos za ostale vrste aplikacija. Korištenje nekog od ovih protokola za stvaranje zaštićenog tunela između dva komunicirajuća subjekta jedna je od važnijih metoda za ostvarivanje računalne sigurnosti. To posebno vrijedi kod web aplikacija jer gotovo svi web preglednici podržavaju SSL protokol pa je zaštita osigurana bez ikakve dodatne konfiguracije ili instalacije aplikacija.

Naslijeđeni sustavi i neosigurane usluge – starim zaštitnim sustavima koji su obično dio štićene aplikacije treba osigurati dodatnu zaštitu. Ovdje se prvenstveno misli na postavljanje vatrozida ili ograničavanje mrežnog prometa korištenjem neke druge tehnike. Također je potrebno isključiti sve suvišne usluge i ograničiti korištenje administrativnih protokola.

Odvajanje usluga je strategija zaštite sustava kojom se nastoji smanjiti broj vidljivih usluga, što je posebice važno kod usluga koje same po sebi nisu zaštićene. Ukoliko su one nužno potrebne, preporuča ih se „sakriti“ iza poslužitelja koji će osigurati korištenje usluge, ali na neki manje ranjiv način. U svakom slučaju nužno je postići smanjenje broja mogućih ulaza za potencijalne napadače.

Konfiguracija osobnih računala možda je najteži od svih sigurnosnih problema, ali se može značajno poboljšati pridržavanjem slijedećih nekoliko pravila:

- Potrebno je koristiti operacijske sustave koji se mogu zaštititi. Ukoliko trenutno korišteni sustav ne pruža dovoljnu razinu zaštite, potrebno je prijeći na drugi.
- Preporuča se korištenje sustava za upravljanje konfiguracijom osobnih računala.
- Preporuča se uporaba tzv. *thin* klijenata (npr. *webPad*) gdje je to prikladno.
- Potrebno je periodički i redovito ispitivati sigurnost proaktivnim provjerama ranjivosti.

2.3. Mrežna sigurnost

2.3.1. Izolacija puteva i VPN

Izolacija puteva je metoda zaštite kod koje se različiti tipovi podataka raspoređuju na različite podatkovne kanale korištenjem prespajanja, virtualnih kanala, enkripcijskih tehnika i različitih fizičkih vodova. Cilj je odvojiti osjetljive podatke od potencijalno opasnog prometa putem kojeg bi napadač eventualno mogao doći do podataka ili ih čak promijeniti. Metode za ostvarenje ovakve zaštite su slijedeće:

- odvajanje fizičkih vodova,
- *Ethernet* odvajanje (izolacija prema MAC adresi),
- odvajanje prema VLAN zastavicama (eng. *tags*),
- MPLS tuneli (odvajanje prema MPLS zastavicama) te
- enkripcija na transportnom sloju (VPN tuneli).

Osim enkripcije na transportnom sloju sve ostale metode odnose se na mrežnu infrastrukturu, a ne na korisničku primjenu.

Odvajanje fizičkih vodova – iako je moguće uspostaviti odvojene fizičke vodove za povezivanje pojedinih poslužitelja, ova metoda ne daje bitne sigurnosne prednosti u usporedbi s metodom enkripcije puteva pa se uglavnom i ne koristi.

***Ethernet* odvajanje** je metoda odvajanja prometa i dijelova mreže *ethernet* preklopnicima čime se kod klijenta postiže dostupnost samo određenog dijela mreže. Međutim i ova metoda ne daje zadovoljavajuću sigurnost jer, ovisno o konfiguraciji, neki *ethernet* preklopnici povremeno mogu propuštati neke pakete na sve priključke. Čak i ako je ispravnom konfiguracijom to spriječeno nije isključena mogućnost napada iz samog odvojka mreže čime bi napadač mogao zavarati preklopnik i proslijediti zlonamjerno oblikovane pakete u druge dijelove mreže.

Odvajanje pomoću VLAN i MPLS zastavica – ovom metodom stvaraju se virtualni odvojeni krugovi kojima se odvajaju podaci na istom fizičkom vodu. Administrator takvog sustava u principu radi mreže unutar mreža označavanjem pojedinih vrsta prometa, a tako dobivena razina sigurnosti slična je onoj prethodno spomenutih metoda.

Odvajanje pomoću enkripcije na transportnom sloju – ovom metodom postiže se dvojaki učinak: odvajaju se različiti tipovi podataka, ali se ujedno i podaci zaštićuju enkripcijom. Metoda je slična enkripciji sjednica SSH ili SSL protokolom s tom razlikom da se ovdje enkripcija ne radi na aplikacijskom sloju nego na transportnom. To znači da se enkripcija događa na samom računalu, tj. unutar njegovog IP stoga a tako zaštićena komunikacija štiti sve aplikacije na tom računalu. Iako je opisana zaštita kompleksnija od SSH ili SSL zaštite ona je vrlo pogodna za zaštitu aplikacija koje ne podržavaju spomenute protokole pa često predstavlja jedino moguće rješenje za zaštitu naslijeđenih aplikacija. Enkripcija na transportnom sloju je osnova na kojoj počiva većina VPN rješenja.

VPN (eng. *Virtual Private Network*) je metoda zaštite koja osigurava odvojeni tunel kroz dio mreže, a u većini implementacija se temelji na enkripciji u transportnom sloju. VPN se primjenjuje u slijedećim situacijama:

- za osiguravanje naslijeđenih aplikacija koje ne podržavaju enkripcijske pristupne protokole (SSH, SSL, Kerberos),
- kada je potrebno osigurati određenu IP adresu udaljenom klijentu (izvan mreže) kako bi se omogućio pristup određenim resursima te
- kada je potrebno ostvariti tunel izvan zaštićene zone (kroz vatrozid) kako bi se klijentima omogućio pristup osjetljivim uslugama.

2.3.2. Zaštita zone

Unatoč pobrojanim metodama zaštite koje bi trebale osigurati pojedina računala i poslužitelje kao i njihovu međusobnu komunikaciju povrh svega se primjenjuje i zaštita na razini cjelokupne mreže, tj. kreira se zaštićena zona. Metode za zaštitu zone su sljedeće:

- filtriranje na usmjerivaču (eng. *Router filtering*),
- NAT (eng. Network Address Translation) u kombinaciji s filtriranjem na usmjerivaču,
- filtriranje na računalu,
- filtriranje specijaliziranim topološkim vatrozidima te
- filtriranje specijaliziranim logičkim vatrozidima.

Točka u kojoj se provodi filtriranje može biti fizički određena lokacijom unutar mreže ili može biti neovisna o fizičkoj lokaciji, ali ovisna o logičkoj lokaciji s obzirom na mrežni promet koji filtrira (virtualni ili logički vatrozidi). I u jednom i drugom slučaju filtriranje se provodi prema jednom ili više slijedećih kriterija:

- broju priključka,
- izvorišnoj adresi,
- odredišnoj adresi,
- statusu veze i
- sadržaju koji uključuje transakcijsko stanje.

Zaštita zone ima dva glavna cilja:

- zaustavljanje dijela prometa ovisno o potrebnim uslugama s ciljem smanjenja broja ulaza u štićeno područje i
- ograničavanje pristupa iz neprovjerenih lokacija s ciljem uspostave zapreka između napadača i mete napada.

3. NAP / NAC sigurnosno rješenje

Kao što je opisano u prethodnom poglavlju važan element računalne sigurnosti je sigurnost osobnih računala, a ona ovisi o njihovoj pravilnoj konfiguraciji koja u velikoj mjeri počiva na samim korisnicima. Međutim nisu svi korisnici jednako odgovorni, a oni neodgovorni predstavljaju prijetnju ne samo vlastitoj sigurnosti nego i sigurnosti svih ostalih. NAP i NAC sustavi nude rješenje za sigurnosni problem neodgovornih korisnika i to tako da na osnovu utvrđene sigurnosti računala unutar mreže reguliraju razinu mrežne sigurnosti.

Princip rada NAP i NAC sustava temelji se na središnjem poslužitelju koji posebnim protokolom ispituje sigurnosno stanje svakog novopriključenog računala i na osnovu utvrđenog stanja poduzima određene sigurnosne mjere. Te se mjere uglavnom sastoje od:

- povećanja razine sigurnosti računala, ukoliko je to moguće, te
- ograničenja pristupa mrežnim resursima dok računalo ne zadovolji sigurnosne zahtjeve.

Kako bi se omogućilo provođenje ovih dviju mjera potrebno je u računalni sustav implementirati neke nove komponente i komunikacijske protokole koji osiguravaju neophodnu infrastrukturu. Kako izgleda ta infrastruktura kod NAP odnosno NAC sustava bit će opisano u slijedećim poglavljima.

4. NAP sustav

NAP sustav predstavlja rješenje za mrežne administratore koje im daje automatske mehanizme prisile korisnika na održavanje svojih računala u skladu s definiranim sigurnosnim pravilima. NAP je proizvod tvrtke Microsoft, a podržavaju ga Windows Longhorn poslužitelj s jedne i Windows Vista klijenti s druge strane. NAP podršku može se osigurati i Windows XP klijentima ako su opremljeni Service Pack 2 zakrpama i NAP klijentom za Windows XP.

NAP sustav ima tri područja djelovanja:

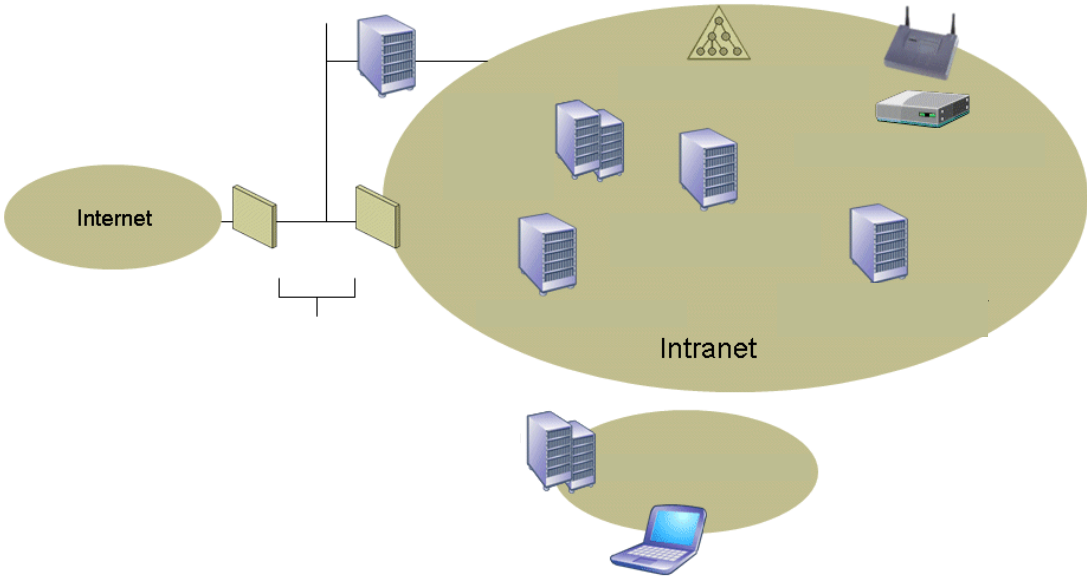
- **Validacija sigurnosnog stanja računala** uključuje provjeru sigurnosnog stanja računala i njegovu usporedbu s definiranom sigurnosnom politikom, prije samog priključivanja na mrežu. Administrator NAP sustava može odrediti koji koraci slijede nakon validacije ako računalo ne zadovoljava sigurnosnu politiku. U okruženju gdje se NAP sustav koristi samo za praćenje sigurnosnog stanja stanje novo-priključenog računala će se samo zabilježiti u

dnevnički zapis za daljnju analizu. U okruženju gdje se NAP sustav koristi i za regulaciju mrežne sigurnosti računalu koje ne zadovoljava sigurnosnu politiku NAP sustav će dati ograničen pristup mrežnim resursima.

- **Provođenje sigurnosne politike** – administratori NAP sustava mogu osigurati provođenje sigurnosne politike tako da se računala koja ne zadovoljavaju politiku nakon provjere automatski nadopune instalacijom potrebnih zakrpi i alata, te da im se promijene konfiguracijske postavke koje osiguravaju traženu razinu zaštite (pomoću upravljačkih aplikacija, npr. *Microsoft Systems Management Server*). U okruženju gdje se NAP sustav koristi samo za praćenje sigurnosnog stanja za vrijeme usklađivanja sa sigurnosnom politikom računalo ima potpuni pristup svim mrežnim resursima, dok u okruženju u kojem se NAP sustav koristi i za regulaciju mrežne sigurnosti nadzirano računalo ima samo ograničen pristup mrežnim resursima, sve dok se ne uskladi sa sigurnosnom politikom. Naravno moguće je definirati i iznimke od ovih pravila za računala koja ne podržavaju NAP sustav zaštite.
- **Ograničenje pristupa** za računala koja nisu usklađena sa sigurnosnom politikom može se ostvariti na dva načina: ograničenjem vremena koje računalo može provesti unutar mreže ili ograničenjem dostupnih mrežnih resursa. U slučaju ograničenja mrežnih resursa NAP administrator određuje resurse kojima takvo računalo može pristupiti, a to je dio mreže putem kojeg se može doći do potrebnih sigurnosnih zakrpi i alata potrebnih za usklađivanje. Moguće je i definirati iznimke kojima se određenim neusklađenim računalima dozvoljava neograničen pristup mrežnim resursima.

4.1. NAP arhitektura

Arhitektura NAP sustava prikazana je na slijedećoj slici.



Slika 1. Arhitektura NAP sustava

Sustav sačinjavaju slijedeće komponente:

- NAP klijent – računalo koje podržava NAP sustav za validaciju sigurnosnog stanja računala i ograničenje mrežnih resursa.
- NAP komponente prisile – komponente sustava koje koriste NAP kako bi provjerile sigurnosno stanje klijenata i na osnovu toga ograničile pristup mrežnim resursima ako sigurnosno stanje nije zadovoljavajuće. NAP komponente prisile koriste NPS (eng. *Network Policy Server*) za validaciju sigurnosnog stanja klijenta i njegovo usklađivanje sa sigurnosnom politikom. NAP komponente prisile opisane su detaljnije u slijedećem poglavlju.

- NPS – poslužitelj ili usluge koje služe za validaciju sigurnosnog stanja klijenata. Ujedno može služiti i kao RADIUS poslužitelj. Detaljnije opisan u slijedećem poglavlju.
- HRA (eng. *Health Registration Authority*) – računalo na kojem se nalazi Windows Longhorn poslužitelj, koje ima osposobljenu IIS (eng. *Internet Information Services*) uslugu i koje generira certifikate za usklađene klijente.
- Poslužitelj sigurnosnih zahtjeva (eng. *Health Requirement Server*) – poslužitelj koji osigurava podatke o trenutnim zahtjevima na sigurnosnu politiku, npr. za antivirusni program to je poslužitelj koji dobavlja najnovije virusne definicije.
- Active Directory usluga – usluga koja služi za pohranjivanje korisničkih identiteta i profila. Nije nužna za provjeru sigurnosnog stanja klijenta, ali se koristi kod nekih metoda prisile.
- Ograničeni mrežni resursi – fizički ili logički odvojen dio mreže koji sadrži:
    - poslužitelje za usklađivanje i
    - NAP klijente s ograničenim pristupom.

Detaljniji opis komponenti NAP sustava dan je u slijedećem poglavlju.

4.2. Komponente NAP sustava

NAP sustav je fleksibilan i može se nadograđivati s novim komponentama koje podržavaju NAP API, ali svaki NAP sustav sadržava nekoliko osnovnih komponenti opisanih u slijedećim poglavljima.

4.2.1. Sigurnosni agent i validator sigurnosti

Sigurnosni agent (eng. *System Health Agents* - SHA) ima ulogu praćenja sigurnosnog stanja računala. Realiziran je kao *Windows Security Health Validator* komponenta unutar Windows Vista, odnosno Windows XP operacijskog sustava. Praćenje sigurnosnog stanja računala provodi provjerom postavki Windows Security centra.

Validator sigurnosti (eng. *Security Health Validator*) realiziran je kao *Windows Security Health Validator* komponenta unutar *Windows Longhorn* poslužitelja, a cilj joj je provjeriti stanje sigurnosti pojedinih računala pomoću podataka dobivenih od pripadnog sigurnosnog agenta.

4.2.2. Komponente i metode prisile

Komponente koje osiguravaju validaciju sigurnosnog stanja i ograničavaju pristup mrežnim resursima nazivaju se klijenti prisile (eng. *Enforcement Clients* – EC) i poslužitelji prisile (eng. *Enforcement Servers* – ES). O načinu pristupa mreži ovisi koji će se klijent prisile koristiti i s kojim će poslužiteljem prisile komunicirati. Operacijski sustavi Windows Vista i Windows XP opremljen sa SP2 i NAP klijentom za Windows XP osiguravaju slijedeće vrste klijenata prisile:

- IPsec (eng. *Internet Protocol security*) klijent prisile,
- IEEE 802.1X klijent prisile,
- udaljeni VPN klijent prisile i
- DHCP klijent prisile.

Windows Longhorn poslužitelji osiguravaju pripadne poslužitelje prisile, a također podržavaju i pristup mreži putem *Terminal Server Gateway* aplikacije. Pobrojane vrste klijenata i poslužitelja prisile implementiraju tzv. NAP metode prisile. Djelovanje svake metode opisano je u nastavku:

- IPsec zaštićeni promet – kod ove metode prisile računalo mora biti usklađeno sa sigurnosnom politikom kako bi moglo komunicirati s drugim računalima. Budući da se radi o IPsec protokolu moguće je definirati zaštitu komunikacije na razini IP adresa ili TCP/IP port ulaza, zbog čega je IPsec najsigurnija NAP metoda za ograničenje pristupa ili komunikacije. Komponente potrebne za realizaciju IPsec metode prisile su *Health Registration Authority* (HRA) kod Windows Longhorn poslužitelja i IPsec klijent prisile na strani računala. HRA generira X.509 certifikate za NAP klijente nakon što se potvrdi njihova usklađenost s politikom, a dobiveni certifikati se koriste za autentikaciju NAP klijenata prilikom iniciranja IPsec veza prema drugim NAP klijentima ili unutar mreže.
- 802.1X pristup – kod ove metode prisile preduvjet za uspostavljanje autenticirane 802.1X veze prema npr. Ethernet poslužitelju za autentikaciju ili prema bežičnoj pristupnoj točki je usklađenost računala sa sigurnosnom politikom. Za neusklađena računala mrežni pristup je

ograničen putem profila ograničenog pristupa koji se definira ili na Ethernet preklopniku ili na bežičnoj pristupnoj točki. Profilom se mogu specificirati ili IP paketni filtri ili identifikatori virtualnih LAN mreža kojima je pristup dozvoljen. Provjera usklađenosti obavlja se prilikom svakog pokušaja dobivanja autenticirane veze, ali se također i aktivno prati sigurnosno stanje već povezanih računala te im se ograničava pristup ako iz nekog razloga postanu neusklađeni. Komponente potrebne za realizaciju 802.1X metode prisile su NPS kao Windows Longhorn poslužitelj i EAPHost klijent prisile na strani računala.

- Udaljeni VPN pristup – svako računalo koje pristupa mreži putem VPN-a za dobivanje neograničenog pristupa mreži mora biti usklađeno sa sigurnosnom politikom. Ograničenje pristupa provodi se pomoću IP paketnih filtara koji se primjenjuju nad VPN vezom od strane VPN poslužitelja. Provjera usklađenosti se obavlja prilikom uspostave veze, ali se aktivno obavlja i kod već povezanih klijenata. Komponente potrebne za realizaciju VPN metode prisile su NPS kod Windows Longhorn poslužitelja i VPN klijent prisile na strani računala.
- DHCP adresna konfiguracija – kod ove metode preduvjet za DHCP konfiguraciju IP adrese je usklađenost sa sigurnosnom politikom. Za neusklađena računala konfigurira se DHCP adresa s kojom je dozvoljen samo ograničen pristup mrežnim resursima. Provjera usklađenosti se obavlja prilikom uspostave veze, ali se aktivno obavlja i kod već povezanih klijenata. Ako se utvrdi neusklađenost obavlja se obnova IP adrese i dodjeljuje se adresa za ograničeni pristup. Komponente potrebne za realizaciju DHCP metode prisile su DHCP poslužitelj prisile koji je dio Windows Longhorn poslužitelja i DHCP klijent prisile na strani računala. Budući da se ova metoda prisile zasniva na konfiguraciji lako promjenjive DHCP adrese s ograničenim pristupom, ona pruža najslabiju zaštitu od svih NAP metoda prisile.

4.2.3. NPS

NPS je komponenta Windows Longhorn poslužitelja koja osigurava RADIUS funkcionalnost, tj. usluge autentikacije, autorizacije i obračuna (eng. AAA – A*uthentication, Authorization, Accounting*). Za autentikaciju i autorizaciju NPS koristi Active Directory uslugu kojom verificira identitet korisnika te njegova prava korištenja mrežnih resursa kod VPN i 802.1X pristupa mreži.
NPS također ima ulogu NAP poslužitelja sigurnosne politike (eng. NAP *Health Policy Server*) na kojem administratori definiraju sigurnosne zahtjeve na klijente u obliku sigurnosnih politika. NPS poslužitelji provjeravaju usklađenost sigurnosnog stanja računala prema informacijama dobivenim od klijenata i za neusklađena računala specificiraju koje radnje treba provesti za usklađivanje. Uloga NPS-a kao AAA poslužitelja je neovisna od njegove uloge kao NAP poslužitelja sigurnosne politike

4.2.4. Poslužitelj za usklađivanje

Poslužitelj za usklađivanje sastoji se od poslužitelja, usluga i drugih resursa dostupnih neusklađenim računalima. Takvi resursi su na primjer: DNS poslužitelj, poslužitelj antivirusnih definicija ili poslužitelj sigurnosnih zakrpa. Sigurnosni klijent može komunicirati s poslužiteljem za usklađivanje izravno ili putem neke klijentske aplikacije.

4.3. NAP scenariji primjene

NAP je pogodan za primjenu u sljedećim scenarijima:

- Verificiranje sigurnosnog stanja putujućih prijenosnih računala – prijenosna računala koja se koriste izvan domicilne mreže nisu nužno uvijek u skladu s definiranom sigurnosnom politikom, a dodatno mogu biti zaraženi nekim virusom za vrijeme korištenja izvan mreže. Prilikom ponovnog ulaska u domicilnu mrežu NAP sustav će provjeriti sigurnosno stanje računala i uskladiti ga sa trenutno propisanom sigurnosnom politikom
- Verifikacija sigurnosnog stanja stolnih računala – iako stolna računala rijetko napuštaju mrežu ona mogu biti zaražena tijekom rada. NAP sustav omogućava automatiziranu provjeru sigurnosnog stanja računala i usklađivanje sa sigurnosnom politikom koje ne ovisi o samom korisniku. Isto tako, NAP sustav omogućava automatizirano usklađivanje računala sa sigurnosnom politikom u situacijama kad se sigurnosna politika unutar mreže promijeni.

- Verifikacija sigurnosnog stanja gostujućih prijenosnih računala – postoje situacije u kojima se dozvoljava privremeni priključak vanjskih prijenosnih računala na mrežu (npr. za rad konzultanata). I za takva računala potrebno je obaviti provjeru sigurnosnog stanja. Međutim u slučaju kada takva računala ne zadovoljavaju sigurnosnu politiku neće se pristupiti automatskom usklađivanju nego će se samo ograničiti pristup mrežnim resursima. U takvoj situaciji moguće je npr. ograničiti pristup tako da računalo može komunicirati samo s javnim Internetom.
- Verifikacija stanja vanjskih računala – priključivanje na mrežu može se dozvoliti i vanjskim računalima putem VPN veze. Budući da administratori mreže nemaju pristup takvim računalima, ona vjerojatno nisu usklađena sa sigurnosnom politikom. Korištenjem NAP sustava administratori im mogu ograničiti pristup mrežnim resursima sve dok se ne usklade sa sigurnosnom politikom.

Ovisno o potrebama, NAP se može konfigurirati za bilo koji od ovih scenarija ili za sve njih.

5. NAC sustav

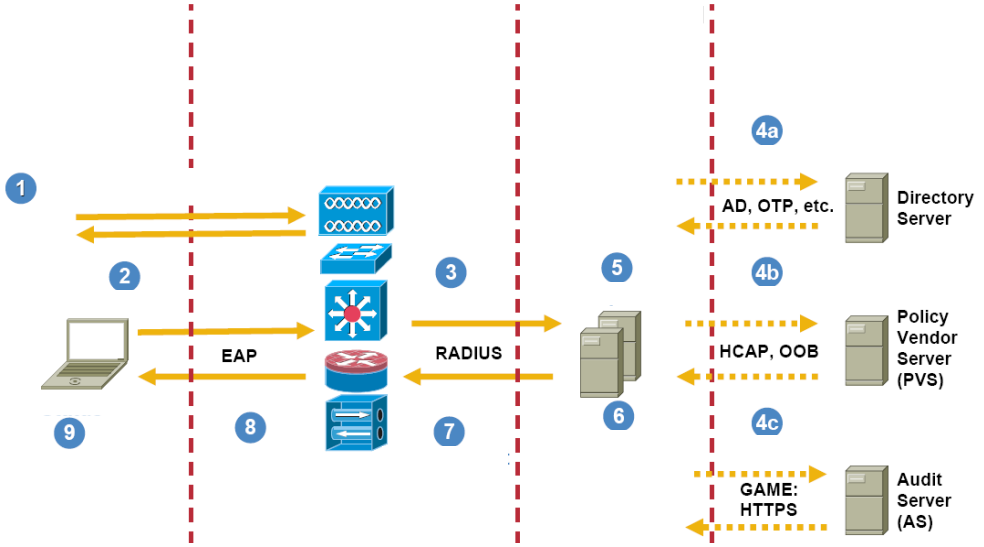
Za razliku od NAP sustava koji je čisto programsko rješenje, NAC se temelji na sklopovlju tvrtke Cisco. Ova tvrtka također osigurava i klijentske aplikacije koje se mogu besplatno preuzeti s njihove stranice. Princip djelovanja NAC sustava zasniva se na ista tri područja:

- provjeri sigurnosnog stanja klijenata prilikom priključivanja na mrežu,
- usklađivanju sa sigurnosnom politikom i
- ograničenju pristupa neusklađenim klijentima.

Realizacija sustava opisana je u slijedećim poglavljima.

5.1. NAC arhitektura

Arhitektura NAC sustava prikazana je na slijedećoj slici.



Slika 2. Arhitektura NAC sustava

NAC sustav strukturno je podijeljen na četiri cjeline:

- Klijenti – računala koja pristupaju mreži te moraju biti opremljena *Cisco Trusted Agent* (CTA) klijentskom aplikacijom koji osigurava podršku za NAC uslugu.
- Pristupne točke – rubne točke mreže putem kojih klijenti pristupaju, a mogu biti uobičajene 802.1X bežične pristupne točke ili IP pristupne točke. U svakom slučaju moraju biti nadograđene za NAC podršku.

- ACS (eng. *Access Control Server*) – poslužitelj kontrole pristupa je točka na kojoj se postavljaju zahtjevi za usklađivanjem i određuju ograničenja pristupa koja pristupne točke primjenjuju.
- Sigurnosna politika – dio sustava koji osigurava infrastrukturu za provođenje sigurnosne politike. Sastoji se od poslužitelja za verifikaciju i podataka koji definiraju potrebne sigurnosne postavke.

Interakcija klijenta i NAC sustava započinje kod prvog zahtjeva klijenta za priključak na mreži. U tom trenutku pristupna točka mreže koja je nadograđena podrškom za NAC zahtijeva provjeru sigurnosnog stanja klijenta. CTA klijentska aplikacija šalje podatke o sigurnosnom stanju klijenta koji se zatim prosljeđuju poslužitelju kontrole pristupa, a on potvrđuje korisnikov identitet i dohvaća informacije o njegovom profilu od *Directory Server* komponente. Nakon verifikacije identiteta korisnika i njegovog profila provjerava se usklađenost korisnika s definiranom sigurnosnom politikom. Podaci o trenutno aktivnoj sigurnosnoj politici dohvaćaju se iz *Policy Vendor Server* komponente. Tom provjerom utvrđuje se sigurnosno stanje klijenta koje može biti sljedeće:

- *Healthy* – klijent je usklađen i nema ograničenja pristupa.
- *Checkup* – klijent nije potpuno usklađen, te je potrebno osvježavanje zakrpa.
- *Transition* – klijent je u procesu usklađivanja te mu je odobren privremen pristup mrežnim resursima do završetka usklađivanja kada slijedi ponovna provjera.
- *Quarantine* – klijent nije usklađen te mu je ograničen pristup mreži. Klijent nije prijetnja, ali predstavlja rizik za sigurnost mreže.
- *Infected* – klijent je zaražen i predstavlja aktivnu prijetnju sigurnosti mreže. Pristup mreži je vrlo ograničen ili potpuno uskraćen.
- *Unknown* – nemoguće utvrditi sigurnosno stanje klijenta. Klijent se stavlja karantenu dok se ne utvrdi njegovo sigurnosno stanje.

Na osnovu sigurnosnog stanja ACS prosljeđuje zahtjeve za ograničenjem pristupa pristupnim točkama koje ga onda svaka na svoj način primjenjuju i o tome obavještavaju klijenta. Ukoliko je potrebno klijent nakon toga provodi usklađivanje i nastavlja s normalnim radom.

5.2. NAC komponente i protokoli

NAC se temelji na nekoliko osnovnih komponenti:

- CTA (eng. *Cisco Trusted Agent*) – klijentska aplikacija koji omogućava razmjenu podataka potrebnih za implementaciju NAC sustava. Klijentima koji nisu opremljeni s CTA aplikacijom pristup mreži može se omogućiti samo konfiguracijom iznimki na osnovu IP ili MAC adresa ili na osnovu tipa uređaja, ali administrator NAC sustava mora svjesno prihvatiti taj rizik.
- Pristupne točke (eng. *Cisco Network Access Device* – NAD) – uobičajene Cisco pristupne točke nadograđene podrškom za NAC sustav. NAC sustav ne radi s pristupnim točkama koje je proizveo netko drugi. Podržane metode pristupa su:
  - NAC L2 IP – IP pristupne točke koje informacije o sigurnosnom stanju razmjenjuju putem EAP povrh UDP protokola. Ocjena sigurnosnog stanja inicira se prilikom bilo kojeg novog ARP zahtjeva ili DHCP povezivanja, dok se ograničenje pristupa provodi pomoću ACL (eng. *Access Control List*) listi koje se dobivaju od AAA poslužitelja.
  - NAC 802.1X – 802.1X pristupne točke koje informacije o sigurnosnom stanju razmjenjuju putem EAP-FAST protokola. Ocjena sigurnosnog stanja inicira se prilikom 802.1X dijaloga kontrole pristupa dok se ograničenje pristupa provodi na pristupnoj točki.
- ACS (eng. *Access Control Server*) – poslužitelj kontrole pristupa. To je komponenta zadužena za provođenje autentikacije. ocjenu sigurnosnog stanja klijenta i definiranje ograničenja pristupa za klijente na pristupnim točkama.
- Directory Server – komponenta za autentikaciju i autorizaciju korisnika koja pohranjuje identitete korisnika i njihove profile. Realizirana je kao Active Directory ili slična usluga.
- PVS (eng. *Policy Vendor Server ili Posture Validation Server*) – poslužitelj za validaciju sigurnosnog stanja klijenta. Ova komponenta može biti proizvod tvrtke Cisco ili drugog proizvođača. Ona pohranjuje podatke o sigurnosnoj politici u određenom formatu i prema

tome obavlja ocjenu sigurnosnog stanja klijenata. Proces ocjenjivanja obavlja se putem HCAP (eng. *Host Credential Authorization Protocol*) protokola unutar HTTP ili HTTPS sjednice.

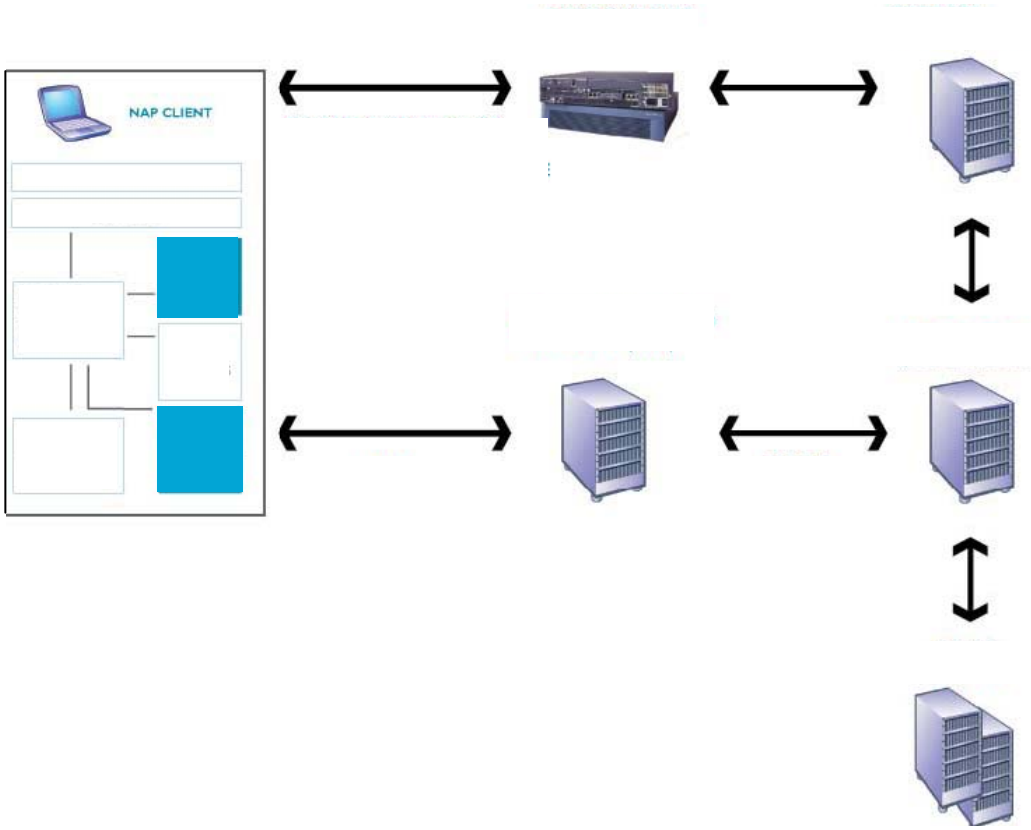
- Audit Server – poslužitelj koji obavlja periodičke kontrole sigurnosnog stanja klijenata koji su već povezani u mrežu i na osnovu novoutvrđenog stanja može uzrokovati promjene ograničenja pristupa. Provjera sigurnosnog stanja klijenta provodi se putem GAME (eng. *Generic Authorization Message Exchange*) protokola unutar HTTPS sjednice.

5.3. NAC područje primjene

NAC područje primjene istovjetno je području primjene NAP sustava, a radi se o ocjeni sigurnosnog stanja prijenosnih, gostujućih, stolnih i udaljenih računala. Sa strane klijenata nema ograničenja na primjenu NAC sustava, ali infrastruktura mora biti većim dijelom temeljena na proizvodima tvrtke Cisco čime ona štiti svoje klijente od konkurencije.

5.4. NAC i NAP interoperabilnost

Uočivši da se radi o sličnim proizvodima, a vođeni proširenjem tržišta, Cisco i Microsoft su se odlučili integrirati svoja dva sustava tako da mogu koegzistirati unutar iste mreže. Tako je Microsoft-ov NAP klijent nadograđen s podrškom za NAC protokole dok je Cisco-ov ACS poslužitelj prilagođen komunikaciji s NAP NPS poslužiteljem za verifikaciju sigurnosnog stanja klijenta. Krajnji rezultat je arhitektura prikazana na slijedećoj slici:



Slika 3. Arhitektura NAP / NAC interoperabilnosti

EAP-FAST ili

SHA agenti

NAP agent

6. Zaključak

NAP i NAC sustavi definitivno donose poboljšanje sigurnosti računalnih mreža jer objedinjuju metode sigurnosne zaštite iz sva tri bitna područja – operativne sigurnosti (sigurnosna politika) sigurnosti aplikacija i računala (sigurnosne zakrpe, autentikacija, konfiguracija računala) i mrežne sigurnosti (ograničen pristup mrežnim resursima za neusklađena računala). Osim toga ovim sustavima se gotovo potpuno eliminiraju posljedice korisničkih pogreški u konfiguraciji i održavanju računala kao i korisnikova nemarnost. Cjelokupni učinak je eliminacija unutarnjih sigurnosnih prijetnji, što uz pravilnu zaštitu od napadača izvana može osigurati vrlo visoku razinu zaštite.

S druge strane za implementaciju bilo kojeg od opisana dva sustava potrebno je nadograditi postojeću infrastrukturu ili je nadopuniti nekim potpuno novim komponentama: Windows Vista poslužitelj, NAP klijent, NPS poslužitelj za NAP; *Cisco Trusted Agent*, ACS poslužitelj, Cisco nadogradnje za pristupne točke za NAC i sl. Posljedica toga je velika cijena implementacije koja odbija korisnike sve dok im postojeća infrastruktura odolijeva sigurnosnim prijetnjama. Baš zbog toga ni jedan od ova dva sustava zasad nije u široj upotrebi, ali obzirom na prednosti koje donose, očekuje se da će ovakva rješenja s vremenom postati standard u većini korporativnih mreža.

7. Reference

[1] Network security, http://staff.washington.edu/gray/papers/credo.html , ožujak 2002.

[2] NAP, http://www.microsoft.com/technet/network/nap/default.mspx, lipanj 2007.

[3] NAP, http://www.microsoft.com/technet/network/nap/naparch.mspx , travanj 2007.

[4] NAC, http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html, 2006.

[5] NAC, www.interop.com/lasvegas/exhibition/interoplabs/nac/CISCONAC.pdf, svibanj 2006.

[6] NAC – NAP interworking, http://www.cisco.com/application/pdf/en/us/guest/netsol/ns617/c654/cdccont_0900aecd8051fc24.pdf , rujan 2006.