Best practice for packet filtering

Ovaj dokument sadrži preporuke za filtriranje IPv4 saobra?aja u AMRESu.

AMRES BPD 110

AMRES BPD no	110
Version	1
Status	Završen (usledi?e još jedna revizija nakon usvajanja Pravilnika o filtriranju saobra?aja u AMRESu)
Date	30.5.2010
Title	Best practice for packet filtering
Working group	Security
Responsible	AMRES/RCUB/UNIC
Category	Recommendation

Rezime (Abstrakt)

Cilj ovog dokumenta je da ponudi pravila za filtriranje saobra?aja u krajnjim institucijama, imaju?i u vidu skup naj?eš?e koriš?enih servisa u tim mrežama.

Svaka institucija ?lanica AMRES mreže bi trebalo da, na perimetru svoje mreže, samostalno kontroliše dolazni i odlazni saobra?aj po pravilima uskla?enim sa važe?im pravilima u AMRESu i upotrebom tehnologije po sopstvenom izboru. Praksa je pokazala da primena minimalnog skupa dobro odabranih pravila za filtriranje saobra?aja, može zna?ajno da umanji broj sigurnosnih incidenata u jednoj mreži. U krajnjem, primena preporuka iz ovog dokumenta, trebalo bi da podigne nivo bezbednosti i efikasnost filtriranja saobra?aja u celom AMRESu.

U dokumentu su navedene karakteristike saobra?aja za naj?eš?e koriš?ene servise u lokalnim mrežama i preporuke za podešavanje odgovaraju?ih paketskih filtara. Opisani su razli?iti postupci razvoja i primene paketskih filtara i predstavljene prednosti i mane njihove implementacije. Na kraju su dati primeri koji ilustruju primenu preporuka i delovi konfiguracionih fajlova, uklju?uju?i komande za paketske filtere na IOS operativom sistemu.

Dokument je namenjen prvenstveno IT osoblju u krajnjim insituticijama, koje u?estvuje u izradi i implementaciji pravila filtriranja.

Uvod

Veliki broj radnih stanica, servera i drugih ure?aja u AMRES mreži je svakodnevno izložen negativnim uticajima, kako unutar same AMRES mreže, tako i sa Interneta. Zbog toga se pred AMRES administratore mreža postavlja zadatak, da omogu?e normalno funkcionisanje svoje mreže, a da sa druge strane, maksimalno onemogu?e negativne uticaje na njih. Pored toga, potrebno je onemogu?iti i širenje negativnih uticaja sa mreže za koju je odgovoran AMRES administrator, ka ostalim mrežama unutar AMRES mreže, kao i na Internet.

Praksa je pokazala da primena minimalnog skupa dobro odabranih pravila za filtriranja saobra?aja može zna?ajno umanjiti broj sigurnosnih incidenata u jednoj mreži.

Cilj ovog dokumenta je da administratore koji upravljaju mrežama, upozna sa osnovnim pravilima i praksom filtriranja naj?eš?e koriš?enih servisa u AMRES-u. Opisan je postupak razvoja i primena paketskih filtara u krajnjim institucijama/organizacijama.

Važno je napomenuti da dokument ne sadrži zahteve ka institucijama/organizacijama. Dokument sadrži isklju?ivo preporuke, i ne obavezuje pojedina?ne institucije/organizacije da ih primene. U tom smislu dokument je pravljen sa ciljem da opiše postupke u razvoju i primeni paket filtera, a ne da bude iscrpan i potpun u opisu naj?eš?e koriš?enih sevisa. U krajnjem, primena preporuka iz ovog dokumenta, treba da podigne nivo bezbednosti i efikasnost filtriranja saobra?aja u AMRES mreži.

Sva pravila se mogu implementiranih na ruterima i/ili firewall ure?ajima. Time se ne isklju?uje primena i drugih tehnologija.

Preporu?ujemo da predhodno pogledate sadržaj dokumenta AMRES BPD 102 „Filtriranje saobra?aja – uvid u tehnologije i mesta njihove primene u AMRESu”, u kome su opisane raspoložive tehnologije filtriranja saobra?aja, a razmatrana je i njihova upotreba i preporuke za primenu u okviru hijerarijske strukture AMRES mreže.

?etiri polazne preporuke za filtriranje saobra?aja

Da bi se smanjile sigurnosne pretnje u nekoj mreži, koriste se razli?iti ure?aji, tehnologije i tehnike za filtriranje saobra?aja. Svaka institucija/organizacija koja želi da poboljša efikasnost filtriranja i nivo bezbednost svoje mreže, treba da primeni slede?e preporuke:

1. Da definiše pravila (a najbolje bi bilo usvojiti pravilnik) o filtriranju saobra?aja (packet filtering/firewall policy), kojima ?e biti odre?eno kako se reguliše protok dolaznog i odlaznog saobra?aja na mreži.
2. Da se u skladu sa zahtevima i potrebama opredeli za tehnologiju filtriranja saobra?aja koju ?e da

implementira.
3. Da na izabranoj tehnologiji, izvrši implemenatciju definisanih pravila i uskladi ih sa performansama ure?aja.
4. Da održava sve komponente rešenja, što uklju?uje ne samo ure?aje, ve? i pravilnik.

Važno je primetiti da se ove preporuke mogu primeniti u bilo kojoj organizaciji, pa i u AMRESu kao celini.

Dokument AMRES BPD 102 „Filtriranje saobra?aja – uvid u tehnologije i mesta njihove primene u AMRESu" je pripremljen da podrži implemenatciju preporukom broj 2, dok je AMRES BPD 110 „Filtriranje saobra?aja u krajnjim institucijama" pripremljen u vezi sa implementacijom preporukama 1 i 3 u krajnjim institucijama.

Proces definisanja i implementacije pravila o filtriranju saobra?aja

Definicije korištenih pojmova

Perimetar mreže institucije ?lanice AMRES-a – nalazi se na vezi pojedine institucije/organizacije i regionalnog servisnog centara kome pripada i na koji je povezana. U odnosu na ovu poziciju se definiše termin odlazni i dolazni saobra?aj.

Odlazni saobra?aj – saobra?aj koji generiše resurs iz interne mreže AMRES ?lanice u pokušaju pristupa eksternoj usluzi. Alternativni termini za odlazni saobra?aj su izlazni ili egress saobra?aj.

Dolazni saobra?aj – saobra?aj koji generiše eksterni resurs u pokušaju pristupa usluzi (servisu) u internom delu AMRES ?lanice. Alternativni termini za dolazni saobra?aj su ulazni ili ingress saobra?aj.

Ve? uspostavljen saobra?aj – saobra?aj iniciran sa resursa iz interne mreže u pokušaju pristupa eksternoj usluzi, koji, u slu?aju upotrebe TCP protokola, omogu?ava uspostavljanje pravila o propuštanju povratnih paketa (reply packet), a blokiranju svih ostalih paketa. Termin je vezan za statefull packet inspection proces na firewall ure?ajima. Alternativno se koristi i termin „ve? uspostavljen saobra?aj".

Filtrirati saobra?aj – da ili ne

Svaka institucija ?lanica AMRES mreže bi trebalo da, na perimetru svoje mreže, samostalno kontroliše dolazni i odlazni saobra?aj po važe?im pravilima u AMRESu, koja mogu biti proširena definisanjem sopstvenih pravila i upotrebom tehnologije po sopstvenom izboru. To, od institucija/organizacija ?lanica AMRESa, zahteva izvesno angažovanje na ovim aktivnostima, u

procesu definisanja i konfigurisanja, a kasnije i održavanja pravila u formi paketskih filtara.

Kada shvate da im proces održavanja paketskih filtara uzima dosta radnog vremena, administratori u nau?noistraživa?kim i obrazovnim ustanovama, ionako ve? preotere?eni poslom, pri definisanju pravila filtriranja primenjuju razli?ite “pre?ice” (npr. otvaranje svih portova za odre?eni skup IP adresa itd.). Ovaj pristup samo prividno olakšava proces konfiguracije i održavanja paketskih filtera. “Pre?ice” ?esto dovode do ve?e ranjivosti lokalne mreže na razli?ite sigurnosne pretnje koje se pojavljuju iz spoljnjeg sveta, što dalje zahteva dodatno angažovanje na oklanjanju posledica nastalih sigurnosnih incidenata.

Praksa je pokazala da primena minimalnog skupa dobro odabranih pravila za filtriranja saobra?aja na perimteru mreže, može zna?ajno umanjiti broj sigurnostnih incidenata u toj mreži.

Osnovna konfiguracija

Inicijalno, definisanje i implementacija pravila filtriranja ne bi trebalo da bude složen postupak. Objasnit ?emo ga na primeru najjednostavnije, ali i najrasprostranjenije konfiguracije u AMRESu - na perimetru mreže institucije se koristi ruter (ili neki drugi L3 mrežni ure?aj) na kome želimo implementirati pravila filtriranja. Cilj je posti?i smanjenje sigurnosnih pretnji na interne resurse u mreži, a da se pri tome zadrži transparentnost servisa za korisnike.

Proces definisanja pravila filtriranja zahteva da se inicijalno odrede bar dve grupe servisa: grupa servisa koji su raspoloživi korisnicima u mreži. Oni bi trebalo da ?ine skup (apsolutno) dozvoljenih servisa. Drugu grupu ?ine servisi koji sa sobom nose odgovaraju?e sigurnosne pretnje.

Predlog skupa (apsolutno) dozvoljenih servisa može se na?i u dodataku A ovog dokumenta, koji je dostupan samo na srpskom jeziku u on-line verziji dokumenta na AMRES wikiju. Preuzet je iz nacrta Pravilnika o filtriranju saobra?aja u AMRES mreži, u kome je pored ostalog definisan minimalan skup pravila koje ?e institucije AMRES-a morati da primene, kako bi se obezbedio zadovoljavaju?i stepen zaštite u mreži. Svi predlozi su do usvajanja pravilnika, a i naknadno podložni izmenama.

Slede?i važan korak je opredeljivanje za strategiju “dozvoli sve” ili “zabrani sve” u razvoju paketskog filtra, definisanju i dodavanju pravila.

Paketski filtri bazirani na “dozvoli sve” vs. “zabrani sve”

Postoje dva osnovna pristupa koja bitno uti?u na proces razvoja paketskog filtra i definisanje pravila:

- **Pristup “dozvoli sve”** (default permit) – podrazumeva da su svi servisi koji nisu eksplicitno zabranjeni, dozvoljeni.
- **Pristup “zabrani sve”** (default deny) – podrazumeva da su svi servisi koji nisu eksplicitno dozvoljeni, zabranjeni.

Obe navedene strategije zahtevaju da administrator definiše skup servisa koji ?e u slu?aju strategije “dozvoli sve” biti zabranjeni, a u slu?aju strategije “zabrani sve” biti dozvoljeni.

Izbor strategije filtriranja saobra?aja koju ?e neka institucija da primeni je važan korak pri razvoju paketskog filtra. Opredeljivanje za jednu ovih strategija ima direktan uticaj na nivo bezbednosti u mreži date institucije.

Praksa pokazuje da je ve?ini administratora lakše da se opredele za strategiju “dozvoli sve” i da definišu servise koje ?e da zabrane, a da svi ostali servisi budu dozvoljeni. Izbor ove strategije, olakšava upravljanje i održavanje samog paketskog filtra, jer nema naknadnih zahteva korisnika za otvaranjem novih portova i dopuštanjem novih servisa. Me?utim, ova strategija pruža niži stepen sigurnosti u mreži u odnosu na pristup “zabrani sve”.

Strategija “zabrani sve” pruža viši nivo bezbednosti i zbog toga se ona preporu?uje za implementaciju u svim krajnjim institucijama AMRESa. Da bi svi servisi, važni za krajnje korisnike i rad same institucije, bili prepoznati i dozvoljeni pri definisanju filtra, korištenje pristupa “zabrani sve” zahteva od administratora ve?u pripremljenost i bolje poznavanje svih raspoloživih resursa u mreži (ne samo mrežne infrastruktre, ve? i servisa koji se u njoj koriste).

ICmyNet.Flow je alat koji može pomo?i administratorima u AMRES ?lanicama, da bolje upoznaju strukturu saobra?aja u svojoj mreži i utvrde na?in na koji se pojedina?ni servisi koriste u njihovoj mreži. Ovaj alat je besplatan za sve akademske institucije i za njegovu implementaciju se možete obratiti na e-mail adresu helpdesk@rcub.bg.ac.rs.

Iterativni postupak implementacije paketskog filtara baziranog na pristupu “zabrani sve”

Poznavanje skupa naj?eš?e koriš?enih servisa je od velike važnosti i omogu?ava neometano funkcionisanje mreže i nakon primene paketskog filtra. Ipak, može se o?ekivati da neki re?e koriš?en servis bude nenamerno izostavljen. **Logovanje podataka o saobra?aju** je svima dostupan mehanizam, koji pruža nezamenljivu pomo? u definisanju pravila filtriranja. U slu?aju, da se neki servis i zaboravi pri definisanju pravila, logovanje može pomo?i da se to prepozna i da se izostavljeni servis naknadno doda u listu dozvoljenih servisa.

Implementacija paketskog filtera podrazumeva slede?e korake:

- U paketski filter inicijalno treba ubaciti pravila filtriranja za sve servise koji su prepoznati kao apsolutno dozvoljeni.
- Na kraju liste pravila, umesto “default deny“ komande dodati pravilo koje dozvoljava sav ostali sobra?aj, i pri tome loguje sve pakete koji su prošli kroz filter primenom ovog pravila. Po okon?anju postupka, na kraj liste treba vratiti pravilo koje blokira sav saobra?aj koji nije prethodnim pravilima dopušten. Time, se vra?a i mogu?ost da nekim korisnicima ne?e raditi odre?eni servisi, jer u ve?ini slu?ajeva postoje re?e koriš?eni servisi koji u prvoj iteraciji nisu prepoznati kao apsolutno dozvoljeni.
- Nakon odre?enog vremenskog intervala, na serveru za logovanje ?e se formirati log fajl, u kome se

mogu prona?i pokušaji pristupa svim servisima, koji nisu predhodno definisani kao apsolutno dozvoljeni, ako takvi pokušaji postoje.
- Pregledati log fajl i identifikovati saobra?aj koji bi trebalo dodati na listu apsolutno dozvoljenih servisa. Proširiti skup pravila za paketski filtar i uklju?iti ovako identifikovane servise. Nakon toga, u log fajlu ne bi više trebalo da se pojavljuju informacije za novododate servise.
  Ako u log fajlu postoji previše zapisa koji poti?u od nekorisnog saobra?aja (npr. skeniranja mreže), tokom uspostavljanja paketskog filtra može biti teško prona?i karakteristi?an saobra?aj za koji ste stvarno zainteresovani. Tada je potrebno blokirati odnosno filtrirati ometaju?i saobra?aj (noisy traffic) uklju?ivanjem posebnog pravila, kako bi se izbeglo upisivanje paketa (koji prolaze kroz filter primenom ovog pravila) u log fajl.

- Kada je identifikovana ve?ina apsolutno dozvoljenih servisa, može se promeniti poslednje pravilo u filteru - u pravilo koje sav ostali saobra?aj blokira.
- I dalje, treba biti spreman na situaciju da neki servis ne?e funkcionisati, jer jako je teško odjednom prepoznati sve servise koji bi trebalo da budu dozvoljeni. U tome slu?aju ponoviti predhodni postupak, i utvrditi o ?emu se radi, odnosno da li neki servis koji je zabranjen, bi trebalo da bude dozvoljen.

Opšte preporuke:

- Pri implementaciji osmišljenih pravila filtriranja, ne treba zaboraviti na dvosmernost komunikacije ve?ine protokola (paketi se u komunikaciji razmenjuju ka obe strane veze). Nema smisla omogu?iti odlazni web saobra?aj iz mreže, ako se ne dozvoli protok paketa koji se vra?aju kao odgovor.
- Tako?e, dobra je praksa voditi ra?una i o imenovanju skupa pravila koja se implementiraju. Ime paketskog filtra bi trebalo da ukazuje na njegovu namenu, mesto primene i da na prvi pogled olakša njegovo razumevanje.
- Pisanje komentara pri definisanju paketskog filtera je tako?e jako zna?ajno. Pravila u paketskom filteru mogu biti teška za razumevanje i naj?eš?e sadrže IP adrese umesto imena nekog mrežnog resursa. Zbog toga, pisanje komentara koji objašnjavaju pojedina pravila, može zna?ajno olakšati razumevanje definisanih pravila, pri njihovom ponovnom pregledu.

Naprednije konfiguracije

Svi naredni koraci u odbrani mreže od spoljnih uticaja zahtevaju segmentaciju mreže, odnosno razdvajanje internih resursa u razli?ite sigurnosne zone, za koje je potrebno obezbediti razli?ite nivoe sigurnosti. Protok saobra?aja iz jedne u drugu sigurnosnu zonu je potrebno regulistati odgovaraju?im skupom pravila. Samim tim, implementacija ovog rešenja zahteva primenu nešto složenenijih pravila za filtriranje saobra?aja.

Mreža mora biti podeljena na mrežne segmente, a za svaki pojedini mrežni segment mora biti definisano kojoj sigurnosnoj zoni pripada. U odgovaraju?em najjednostavnijem, ali i ?esto korištenom rešenju - na perimetru mreže institucije se nalazi firewall na kome su implementirana pravila filtriranja saobra?aja izme?u tri sigurnosne zone.

Insitucije ?lanice AMRESa koje odlu?e da koriste firewall ure?aj, sem interne i eksterne zone, treba da uvedu minimalno još jedu zonu, tj. **demilitarizovanu zonu** (Demilitarised zone – **DMZ**).

- DMZ zona se uvodi da bi se izolovali servisi kojima se pristupa spolja (preko eksternih veza institucije). Time se za ove servise može obezbediti i dodatna zaštita. Servisi pogodni za odvajanje u DMZ zonu su web stranice i portali, webmail servis, eksterni DNS serveri, VPN servis i sli?no.
- Interna zona je rezervisana za mrežne segmente (jedan ili više njih) kojima ne bi trebalo da bude omogu?en pristup direktno sa mašina koje se nalaze van institutucije.

Pristup servisima u svakoj zoni mora biti pod kontrolom odogovaraju?ih sirunosnih pravila, odnosno paketskog filtra. Institucije mogu primeniti paketske filtre bazirane na “dozvoli sve” ili “zabrani sve” (poglavlje 2.4), kao i njihovu kombinaciju. Za pojedine delove mreže se može primeniti jedna strategija filtriranja, a za ostale delove mreže druga. Naj?eš?e se kombinuju sa medotom koja omogu?ava razmena saobra?aja samo za “ve? uspostavljeni veze“.

Prepoznavanje po?etnih paketa, omogu?ava uspostavljanje veza koje su inicirane iz interne mreže pri pristupu spoljašnjem servisu, ali ne i obrnuto. Dakle, po?etni paket se prihvata za odlazni saobra?aj iz interne zone, dok se odbija za dolazni saobra?aj. Primenom ovog metoda, dalja razmena saobra?aja se omogu?ava samo za “ve? uspostavljene veze“.

Uspostavljanjem pravila o razmeni saobra?aja izmedju pojedinih zona ne bi trebalo da se naruši minimalni nivo bezbednosti definisan za svaku zonu pojedina?no. Pristup resursima u zoni na višem nivou bezbednosti, iz zona na nižem nivou, bi trebalo biti omogu?eno samo uz specifi?nu dozvolu i proveru. Uz to, nije neophodno da iz odre?ene zone postoji mogu?nost pristupa svim zonama na nižem nivou bezbednosti. Primena preporuke na primeru tri preložene zone je slede?a: pristup iniciran iz interne zone može biti omogu?en ka servisima u DMZ zoni, ali ne nužno i servisima u eksternoj zoni. Pristup resursima u internoj zoni iz DMZ zone može biti dozvoljen uz dodatnu autentifikaciju ili autorizaciju, ne samo primenom pravila o filtriranju saobra?aja.

Preporu?uje se i slede?e:

- U svim zonama, trebalo bi jasno razdvojiti klijente od namjenskih (dedicated) servera. Drugim re?ima, klijenti i serveri trebalo bi da se nalaze na razli?itim segmentima mreže, ?ak i kada ti segmenti pripadaju istoj sigurnosnoj zoni. (Razdvojeni mrežni segmenti u istoj sigurnosnoj zoni mogu imati razli?ita pravila filtriranja saobra?aja, što se vremenom može pojaviti kao potreba.)
- Za posetioce bi trebalo obezbediti pristup mrežni preko posebnog mrežnog segmenta, bilo da je on beži?ni ili kablovski. Svakako, pored posetioca mogu da ga koriste i zaposleni u instituciji kada imaju potrebu da brzo pristupe intenetu. U smislu nivoa bezbednosti, taj segment je jednako nebezbedan kao internet, te bi ga trebalo tako i tretirati.
- Institucija se može odlu?iti da implementira i dodatne sigurnosne zone. Pronalaženje balansa izme?u zahteva za adekvatnom sigurnoš?u i otvorenoš?u same mreže, u mreži nau?noistraživa?kih i obrazovnih ustanova, može biti nešto složeniji zadatak.

Naj?eš?e koriš?eni servisi

U ovom poglavlju, opisan je saobra?aj karakteristi?an za pojedine servise. Analizom je obuhva?en skup naj?eš?e koriš?enih servisa u mrežama krajnjih institucija. Pažnja je posve?ena kontroli dolaznih konekcija, dok su za odlazne konekcije naglašene uglavnom zabrane (kada se preporu?uju).

Objašnjenja su prilago?ena implementaciji preporuka u osnovnoj konfiguraciji (vidi poglavlje 2.3). Kao takva, ne mogu se direktno koristiti u naprednijim konfiguracijama, ali ih je lako prilagoditi konkretnoj konfiguraciji sa sigurnosnim (branjenim) zonama. Za primenu u naprednijim konfiguracijama, u tabelama je istaknuto i kada postoji mogu?nost kontrole saobra?aja preko ACK flega (pogledati objašnjenje u poglavlju 2.6 Naprednije konfiguracije).

Napomena: Poglavlje sadrži isklju?ivo preporuke, koje ne obavezuju pojedina?ne institucije da ih primene. Dakle, tekst ne treba tuma?iti kao zahtev za institucije ?lanice AMRES-a.

SMTP

SMTP (Simple Mail Transport Protocol) je TCP protokol koji služi za prenos pošte izme?u mail servera i izme?u klijenata i mail servera. SMTP server *sluša* na portu 25. Danas, ve?ina servera koristi ESMTP (Extended SMTP) koji takodje koristi port 25.

Ra?unari koji primaju poštu pomo?u SMTP protokola koriste port 25, dok ra?unari koji šalju poštu koriste slu?ajno odabran port iznad 1023.

Direction	Source addr.	Dest. addr.	Protocol	SourcePort	Dest.port	ACK set*	Notes
In	Ext	Int	TCP	>1023	25	**	Incoming mail, sender to recipient
Out	Int	Ext	TCP	25	>1023	Yes	Incoming mail, recipient to sender
Out	Int	Ext	TCP	>1023	25	**	Outgoing mail, sender to recipient
In	Ext	Int	TCP	25	>1023	Yes	Outgoing mail, recipient to sender

* Ukoliko postoji mogu?nost kontrole ACK flega

** ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

Preporuke:

- Identifikovati mail servere u lokalnoj mreži i dozvoliti odlazni mail saobra?aj (slanje pošte) samo sa tih servera, a dolazni mail saobra?aj (prijem pošte) samo na te servere.
  - TCP saobra?aj sa lokalnih mailservera za portove iznad 1023 dozvoljen prema portu 25.
  - Dolazni TCP saobra?aj za portove iznad 1023 dozvoljen ka lokalnim mailserverima na portu 25.
- Odlazni TCP saobra?aj sa ra?unara u lokalnoj mreži (osim za lokalne mailservere) prema portu 25 blokirati u cilju smanjenja emitovanja spam poruka sa inficiranih ra?unara.
- Upotreba externih mail server može biti uslovno opravdana/dozvoljena. Naj?eš?e su to mail serveri

raspoloživi u servisnim centrima AMRESa, npr. afrodita, tesla. (#za amres diskusiju ostaviti: Svaku pojavu pristupa mail serverima izvan AMRESa preko porta 25 bi tebalo obeshrabriti.)
Kada korisnici u lokalnoj mreži imaju potrebu da koriste mail servere van lokalne mreže proveriti da li je dostupan mail servis preko web interfejsa i uputiti ih da ga koriste . Ako ne žele ili imaju naviku/potrebu da pristupaju mail servisu po portu 25, identifikovati externe mail servere koje koriste i ograni?iti konekcije samo na identifikovane servere.
    - TCP saobra?aj sa lokalnih klijentskih ra?unara za portove iznad 1023 dozvoljen prema portu 25 identifikovanih externih server.

- Na lokalnim mail serverima isklju?iti *relay* funkciju.

Standardni SMTP protokol ne vrši enkripciju poruka koje prenosi. Zbog takvog na?ina rada, e-mail saobra?aj je podložan razli?itim vrstama sigurnosnih pretnji. Da bi se to spre?ilo, koristi se SMTP sa TLS/SSL enkripcijom. TLS/SSL enkripcija sa sobom donosi mehanizme koji obezbe?uju da se utvrdi ta?an identitet SMTP servera, obezbedi enkripcija podataka koji se koriste za autentifikaciju klijenata na SMTP serveru (username i password) i zaštiti tajnost samih podataka, u porukama koje se prenose, na putanji od klijentskog ra?unara do SMTP servera.

Upotreba SMTP TLS/SSL protokola je svakako preporuka prilikom slanja e-mail poruka ka serverima van AMRES mreže, ali i prilikom slanja e-mail poruka sa klijenata van AMRES mreže na e-mail servere u AMRES mreži. Na taj na?in su zašti?ene i poruke koje se prenose i podaci koji se koriste za autentifikaciju na samom serveru (username i password). Standardizovani broj porta, za SMTP SSL/TLS komunikaciju je 587. Ovo je odredišni port koji klijenti koriste za slanje podataka ka e-mail serveru.

Primena TLS/SSL enkripcije zahteva instalaciju sertifikata na samom serveru, zahteva dodatnu konfiguraciju e-mail servera i zahteva ve?e hardverske kapacitete (procesorska snaga itd.) samog servera.

POP3/POP3S

POP3 (Post Office Protocol Version 3) je klijent/server protokol za transport pošte od servera do elektronskih poštanskih sandu?i?a (mailboxes).

Pri koriš?enju ovog servisa preko Interneta name?e se osnovno pitanje bezbednosti odnosno mogu?nost otkrivanja lozinke. U komunikaciji izme?u klijenta i servera lozinka se šalje preko Interneta tako da oni koji “osluškuju” komunikaciju mogu da snime lozinku. U ve?ini slu?ajeva POP3 lozinka je ista kao i lozinka koja služi za logovanje na server takoda mogu da dobiju privilegije korisnika na serveru.

Da bi se zaštitili od prisluškivanja POP3 Internet komunikacije koristi se POP preko SSL-a (Secure POP) koji kriptuje celu komunikaciju ali to zahteva upotrebu drugog porta.

Klasi?ni POP3 koristi port 110, dok POP3 preko SSL-a (POP3S) koristi port 995. POP3 klijenti koriste portove iznad 1023.

Direction	Source addr.	Dest. addr.	Protocol	SourcePort	Dest.port	ACK set*	Notes
In	Ext	Int	TCP	>1023	110/995	**	Incoming POP/SSL connection, client to server.
In	In	Ext	TCP	110/995	>1023	Yes	Answer the incoming POP/SSL connection, server to client.
Out	In	Ext	TCP	>1023	110/995	**	Outgoing POP/SSL connection, client to server.
Out	Ext	Int	TCP	110/995	>1023	Yes	Answer the outgoing POP/SSL connection, server to client.

* Ukoliko postoji mogu?nost kontrole ACK flega

** ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

Napomena: Mail server i POP/POP3S server se koriste u paru za slanje/prijem pošte, pa se naziv koristi iteretivno.

Preporuke:

- Identifikovati POP/POP3S servere u lokalnoj mreži sa kojih ra?unari u lokalnoj mreži preuzimaju poštu. Nije poželjno da korisnici preko externih linkova preuzimaju poštu sa lokalnih POP3 servera osim kada za to koriste kriptovane konekcije (POP3S).
  - Dolazni TCP saobra?aj za portove iznad 1023 zabraniti ka lokalnim mailserverima na portu 110.
  - Dolazni TCP saobra?aj za portove iznad 1023 dozvoliti ka lokalnim mailserverima na portu 995.
- Upotreba externih POP/POP3S servera može biti uslovno opravdana/dozvoljena, pri ?emu treba forsirati upotrebu POP3S protokola. Naj?eš?e postoji potreba za pristup POP3S serverima raspoloživim u servisnim centrima AMRESa, npr. afrodita, tesla. (#?da li ostaviti Svaku pojavu pristupa POP/POP3S serverima izvan AMRESa bi tebalo obeshrabriti.)
  - TCP saobra?aj sa lokalnih klijentskih ra?unara za portove iznad 1023 zabraniti prema portu 110 identifikovanih externih server.
  - TCP saobra?aj sa lokalnih klijentskih ra?unara za portove iznad 1023 dozvoliti prema portu 995 identifikovanih externih server.
- Forsirati upotreba POP3S protokola (preduslov je instalacija sertifikata na serverma).

IMAP/IMAPS

IMAP sli?no kao POP3 protokol služi preuzimanje elektronske pošte sa mail servera. IMAP je noviji protokol, pruža ve?u fleksibilnost, uklju?uju?i i podršku za višestruke poštanske sandu?i?e.

IMAP je nebezbedan protokol jer se korisni?ko ime i lozinka prenose kao obi?an tekst odnosno nisu kriptovani. Postoji i verzija IMAP-a preko SSL-a (IMAPS) koja kriptuje celu komunikaciju i koja koristi poseban port.

Klasi?ni IMAP koristi port 143, dok IMAP preko SSL-a (IMAPS) koristi port 993. IMAP klijenti koriste portove iznad 1023.

Direction	Source addr.	Dest. addr.	Protocol	SourcePort	Dest.port	ACK set*	Notes
In	Ext	Int	TCP	>1023	143/993	**	Incoming IMAP/IMAPS connection, client to server.
Out	Int	Ext	TCP	143/993	>1023	Yes	Answer the incoming IMAP/IMAPS connection, server to client.
Out	Int	Ext	TCP	>1023	143/993	**	Outgoing IMAP/IMAPS connection, client to server.
In	Ext	Int	TCP	143/993	>1023	Yes	Answer the outgoing IMAP/IMAPS connection, server to client.

* Ukoliko postoji mogu?nost kontrole ACK flega

** ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

Napomena: Mail server i IMAP/IMAPS server se koriste u paru za slanje/prijem pošte, pa se i naziv koristi iterativno.

Preporuke:

- Identifikovati mail servere (IMAP/IMAPS) servere u lokalnoj mreži sa kojih ra?unari u lokalnoj mreži preuzimaju poštu. Nije poželjno da korisnici preko externih linkova preuzimaju poštu sa lokalnih IMAP servera osim kada za to koriste kriptovane konekcije (IMAPS).
  - Dolazni TCP saobra?aj za portove iznad 1023 zabraniti ka lokalnim mailserverima na portu 143.
  - Dolazni TCP saobra?aj za portove iznad 1023 dozvoliti ka lokalnim mailserverima na portu 993.
- Upotreba externih mail server (IMAP/IMAPS) servera može biti uslovno opravdana/dozvoljena, pri ?emu treba forsirati upotrebu IMAPS protokola. Naj?eš?e postoji potreba za pristup POP3S serverima raspoloživim u servisnim centrima AMRESa, npr. afrodita, tesla. (#?da li ostaviti Svaku pojavu pristupa IMAP/IMAPS serverima izvan AMRESa bi tebalo obeshrabriti.)
  - TCP saobra?aj sa lokalnih klijentskih ra?unara za portove iznad 1023 zabraniti prema portu 143 identifikovanih externih server.
  - TCP saobra?aj sa lokalnih klijentskih ra?unara za portove iznad 1023 dozvoliti prema portu 993 identifikovanih externih server.
- Forsirati upotreba IMAPS protokola (preduslov je instalacija sertifikata na serverima).

HTTP/HTTPS

HTTP (HyperText Transfer Protocol) je osnovni protokol na kome se bazira web i sam po sebi predstavlja relativno siguran protokol. Web klijenti tradicionalno koriste http protokol za

komunikaciju sa web serverima za preuzimanje I slanje podataka bez enkripcije. Za osetljive transakcije razvijeni su HTTPS I SHTTP protokoli koji koriste enkriptovanu komunikaciju izme?u klijenta I servera. HTTPS je kombinacija HTTP protokola I SSL/TLS protokola koji obezbe?uju šifrovanje podataka i ima pre svega za cilj da zaštiti komunikacioni kanal prilikom slanja I preuzimanja podataka. SHTTP ima za cilj pre svega da bolje zaštiti pojedinane objekte nego kanal komunikacije. Ovo omogu?ava, na primer, da pojedina?ne stranice na serveru budu digitalno potpisane.

HTTP saobra?aj se bazira na TCP protokolu. Ve?ina servera koristi port 80 ali ne svi. HTTPS koristi TCP konekcije na portu 443. Secure HTTP je dizajniran da radi preko porta 80. Proxy serveri tradicionalno koriste port 8080.

Direction	Source addr.	Dest. addr.	Protocol	SourcePort	Dest.port	ACK set*	Notes
In	Ext	Int	TCP	>1023	80/443	**	Request, external client to internal server
Out	Int	Ext	TCP	25	>1023	Yes	Response, internal server to external client
Out	Int	Ext	TCP	>1023	25	**	Request, internal client to external server
In	Ext	Int	TCP	25	>1023	Yes	Response, external server to internal client

* Ukoliko postoji mogu?nost kontrole ACK flega

** ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

Preporuke:

- Identifikovati HTTP/HTTPS servere u lokalnoj mreži i dozvoliti dolazni http saobra?aj (pristup web sadržajima) samo na te servere.
  Pravila filtirarnja paketa na nivou AMRESa (AMRES Policy) treba da onemogu?e lokalne administratore da koriste nestandardne portove naro?ito ne one iznad 1023. U cilju uskla?ivanja pravila preporu?uje se da dolazni TCP saobra?aj za portove iznad 1023 bude dozvoljen prema web serverima na portu 80 (443 za https).
  - Dolazni TCP saobra?aj za portove iznad 1023 dozvoljen ka lokalnim HTTP serverima na portu 80.
  - Dolazni TCP saobra?aj za portove iznad 1023 dozvoljen ka lokalnim HTTPS serverima na portu 443.

- Tretman odlaznog HTTP/HTTPS saobra?aja zavisi od Pravila filtriranja institucije/organizacije i odluke institucije/organizacije da koristi proxy servere u lokalnoj mreži. Upotreba internog proxy servera ima prednosti ne samo kada je u pitanju propusni opseg veze, ve? i bezbednost interne mreže.
  U oba slu?aja, potrebno je imati u vidu da Pravila filtirarnja paketa na nivou AMRESa (AMRES Policy) propisuje upotrebu AMRES proxy servera za HTTP/HTTPS i KOBSON servise na nivou AMRESa na na?in opisan u poglavlju #.

- Ako institucija/organizacija ne koristi proxy u lokalnoj mreži, dozvoliti odlazni saobra?aj po portovima 80, 443 (za https) i 8080 (za externi proxy).

- Ako institucija/organizacija koristi proxy u lokalnoj mreži, u cilju uskla?ivanja pravila na razli?itim nivoima, dozvoliti odlazni saobra?aj ka portovu 8080 na proxy serverima u AMRES servisnim centrima. Odlazni saobra?aj po portovima 80 i 443, zavisno od odluke institucija/organizacija može biti dozvoljen ka odredišnim adresama iz AMRES adresnog prostora, ili selektivno za pojedine ra?unare u lokalnoj mreži institucije.

- Pravila filtrirarnja paketa na nivou AMRESa (AMRES Policy) treba da zabrane eksterne konekcije na proxy servere u lokalnoj mreži.

DNS

Generalno posmatrano, ve?ina institucija ima autoritativne DNS (Domain Name System) servere koji odgovaraju za njihov domen. Oni moraju da odgovore na upite sa Internet-a, na rekurzivne upite iz lokalne mreže i da vrše transfer zonskih fajlova.

Zbog brzine, DNS upiti se obi?no izvršavaju koriste?i UDP. Ako se neki od paketa izgubi tokom prenosa upit može biti ponovljen koriš?enjem TCP. Ukoliko DNS transakcija zahteva više podataka nego što se uklapa u UDP paket, DNS može automatski da prebaci konekciju na TCP port umesto UDP.

DNS serveri, standardno, osluškuju na portu 53 za UDP i TCP upite. Uobi?ajeno je da serveri koriste portove iznad 1024 za TCP zahteve. Neki serveri koriste port 53 kao izvorni port za UDP upite, dok drugi koriste port iznad 1023. DNS klijenti koriste slu?ajno izabran port iznad 1023 za UDP i TCP.

Da bi se pokrenuo transfer zone potrebno je da sekundarni DNS uputi zahtev primarnom DNS-u ili da dobije notify poruku od primarnog DNS-a. Zahtev za transferom zone se inicira od sekundarnog DNS-a, UDP protokolom, na slu?ajno odabranom portu iznad 1023 ka primarnom DNS-u na portu 53. Kada se ustanovi potreba za transferom zone, sam transfer se vrši koriš?enjem TCP.

Notify poruke ponašaju se kao standarni upiti izme?u dva servera.

Direction	Source addr.	Dest. addr.	Protocol	SourcePort	Dest.port	ACK set*	Notes
In	Ext	Int	UDP/TCP	>1023	53	***	Query via UDP/TCP, external client to internal server
Out	Int	Ext	UDP/TCP	53	>1023	Yes	Response via UDP/TCP, internal server to external client
Out	Int	Ext	UDP/TCP	>1023	53	***	Query via UDP/TCP, internal client to external server
In	Ext	Int	UDP/TCP	53	>1023	***	Response via UDP/TCP, external server to internal client

In	Ext	Int	UDP	53	53	***	Query or response between two servers via UDP
Out	Int	Ext	UDP	53	53	***	Query or response between two servers via UDP
In	Ext	Int	TCP	>1023	53	**	Query or zone transfer request from external server to internal server via TCP
Out	Int	Ext	TCP	53	>1023	**	Response (including zone transfer response) from internal server to external server via TCP
Out	Int	Ext	TCP	>1023	53	**	Query or zone transfer request from internal server to external server via TCP
In	Ext	Int	TCP	53	>1023	Yes	Response (including zone transfer response) from external server to internal server via TCP

* Ukoliko postoji mogu?nost kontrole ACK flega

** ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

*** UDP ne koristi ACK fleg

Preporuke:

- Identifikovati dns servere u lokalnoj mreži i dozvoliti dolazni dns saobra?aj (upite i zahtev za transfer zone) samo na te servere.
  - Dolazni UDP saobra?aj za port 53 i portove iznad 1023 dozvoljen ka lokalnim dns serverima na portu 53.
  - Dolazni TCP saobra?aj za portove iznad 1023 dozvoljen ka lokalnim dns serverima na portu 53.
- Dozvoliti sav odlazni UDP/TCP saobra?aj sa ra?unara u lokalnoj mreži prema portu 53.
- Poželjno je definisati i koristiti bar jedan externi server kao sekundarni server za domen. Naj?eš?e su to dns serveri raspoloživi u servisnim centrima AMRESa, npr. #dodati koji
- Na primarnom dns serveru ograni?iti funkciju *zone-transfer* i konekcije dozvoliti samo njegovim sekundarnim serverima. Razmena zonskih tabela se može i više osigurati i to upotrebom serverskih sertifikata na dns serverima.

Telnet

Telnet omogu?ava pristup sa udaljenog ra?unara do komandne linije na drugom kompjuteru. Podržan je u skoro svim platformama na Internetu. Telnet komunikacija izme?u ra?unara odvija se u

ne-kriptovanom modu (otvoren tekst) što je osnovni nedostatak ovog servisa.

Telnet serveri koriste port 23, osim u izuzetnim slu?ajevima kada se koristi neki drugi port. Telnet klijenti koriste slu?ajno odabran port iznad 1023.

Direction	Source addr.	Dest. addr.	Protocol	SourcePort	Dest.port	ACK set*	Notes
In	Ext	Int	TCP	>1023	23	**	Incoming session, client to server.
Out	Int	Ext	TCP	23	>1023	Yes	Incoming session, server to client.
Out	Int	Ext	TCP	>1023	23	**	Outgoing session, client to server.
In	Ext	Int	TCP	23	>1023	Yes	Outgoing session, server to client.

* Ukoliko postoji mogu?nost kontrole ACK flega

** ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

Preporuke:

- Forsirati upotrebu SSH umesto Telnet protokola.
- Upotrebu Telnet protokola ograni?iti na lokalnu mrežu, a i tada samo na nekim segmentima mreže ili za pristup ure?ajima koji ne podržavaju druge protokole.
- Izbegaviti svaku upotrebu ovog protokola u komunikaciji van lokalne mreže. Ukoliko to nije mogu?e, poželjno je ograni?iti konekcije sa eksternih linkova ka lokalnim telnet serverima.
  - Dolazni TCP saobra?aj za portove iznad 1023 (sa identifikovanih externih ra?unara) dozvoljen ka lokalnim telnet serverima na portu 23.
- Telnet konekcije od lokalnih klijenata ka eksternim serverima mogu biti dozvoljene.
  - TCP saobra?aj sa lokalnih klijentskih ra?unara za portove iznad 1023 dozvoljene prema portu 23 (#identifikovanih) externih servera.

Secure Shell (SSH)

SSH sli?no kao i telnet omogu?ava remote pristup do komandne linije na drugom kompjuteru. Za razliku od telnet-a komunikacija izme?ju klijenta i servera odvija se u enkriptovanom obliku, zbog ?ega se preporu?uje za primenu umesto telnet protokola gde god je to mogu?e.

SSH serveri koriste port 22. SSH klijenti koriste slu?ajno odabran port iznad 1023, osim u slu?aju kada koriste .rhost-based authentication methods kada mogu da koriste i portove ispod 1024.

Direction	Source addr.	Dest. addr.	Protocol	SourcePort	Dest.port	ACK set*	Notes
In	Ext	Int	TCP	Any ***	22	**	Incoming SSH connection, client to server.
Out	Int	Ext	TCP	22	Any ***	Yes	Incoming SSH connection, server to client.
Out	Int	Ext	TCP	Any ***	22	**	Outgoing SSH connection, client to server.
In	Ext	Int	TCP	22	Any ***	Yes	Outgoing SSH connection, server to client.

* Ukoliko postoji mogu?nost kontrole ACK flega

** ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

*** SSH clients use a port below 1024 when using .rhost-based authentication methods, and a port above 1023 otherwise.

Preporuke:

- Omogu?iti dolazne SSH konekcije samo na SSH servere na portu 22.
  - Dolazni TCP saobra?aj za portove iznad 1023 dozvoljen ka lokalnim SSH serverima na portu 22.
  - Odlazni TCP saobra?aj za portove iznad 1023 dozvoljen ka portu 22.

- Razmisliti o isklju?ivanju funkcije *port forwarding*.

Ping

Ping i druge alate za dijagnostiku mreže koji se baziraju na ICMP protokolu koriste administratori mreža za rešavanje problema na mreži. Ping aplikacija generiše “echo request” paket. Ciljni ure?aj odgovara sa “echo response” paketom. ICMP je uglavnom implementiran u operativni sistem tako da nije potreban poseban server na odredišnom ra?unaru.

ICMP poruke nemaju broj porta ali zato imaju naziv i oznaku poruke. Mnogi sistemi za filtriranje paketa omogu?avaju da filtrirate ICMP pakete navo?e?i tip poruke umesto UDP/TCP portova.

Iako su ping i drugi alati koji se baziraju na ICMP protokolu korisni za dijagnostiku mreže, ICMP protokol se može iskoristiti za napade na ra?unare i druge ure?aje na mreži (DoS attack, ICMP Smurf attack, ICMP Flood attack, Ping of Death attack, …).

Direction	Source addr.	Dest. addr.	Protocol	Message Type	Notes
In	Ext	Int	ICMP	8	Incoming ping
Out	Int	Ext	ICMP	0	Response to incoming ping
Out	Int	Ext	ICMP	8	Outgoing ping

In	Ext	Int	ICMP	0	Response to outgoing ping

Preporuke:

- Omogu?iti odlazni ping saobra?aj (pinging remote hosts), tako što ?e se dozvolite *ICMP echo request* paketima da odlaze ka Internetu (outbound) i *ICMP echo response* paketima da dolaze u vašu mrežu (inbound). Pravila filtirarnja paketa na nivou AMRESa (AMRES Policy) trebalo bi da ograni?e ovu operaciju samo sa ra?unara koje koristi osoblje zaduženo za održavanje mreže.
- Omogu?iti dolazni ping saobra?aj (ra?unari sa Interneta “pinguju” ra?unare u vašoj lokalnoj mreži), tako što ?e se dozvolite *ICMP echo request* paketima da ulaze u vašu mrežu i *ICMP echo response* paketima da odlaze ka Internetu. Ovu operaciju ograni?iti i dozvoliti samo identifikovanim externim hosovima (u AMRES servisnim centrima ili izvan AMRESa), i koristiti za potrebe dijagnostike mreže.
- Ograni?iti veli?inu *ICMP echo request* paketa, kao meru zaštite od pojedinih vrsta ICMP napada.

Network Time Protocol (NTP)

NTP (Network Time Protocol) se koristi za sinhronizaciju vremena na ra?unarima.

NTP serveri koriste UDP port 123 za komunikaciju sa drugim serverima i sa klijentima. NTP klijenti koriste slu?ajno odabran port iznad 1023.

Direction	Source addr.	Dest. addr.	Protocol	SourcePort	Dest.port	Notes
In	Ext	Int	UDP	>1023	123	Query, external client to internal server
Out	Int	Ext	UDP	123	>123	Response, internal server to external client
Out	Int	Ext	UDP	>1023	123	Query, internal client to external server
In	Ext	Int	UDP	123	>123	Response, external server to internal client
In	Ext	Int	UDP	123	123	Query or response between two servers
Out	Int	Ext	UDP	123	123	Query or response between two servers

NTP koristi UDP, pa je osetljiv na IP spoofing.

Strategija filtriranja NTP saobra?aja zavisi od toga gde se nalazi server odnosno serveri koje koriste klijenti unutar vaše lokalne mreže.

Najbolja varijanta je da imate NTP server unutar vaše lokalne mreže koji sinhronizuje vreme pomo?u

GPS ?asovnika ili nekog drugog ure?aja koji ne koristi Internet za sinhronizaciju. Tada možeta da zatvorite portove za NTP saobra?aj (dolazni i odlazni) prema Internetu. Ovo rešenje je retko primenjivo u AMRESu.

Druga varijanta podrazumeva da u okviru svoje mreže imate NTP server koji se sinhronizuje preko interneta a klijenti u okviru vaše mreže koriste usluge samo tog servera. U tom slu?aju treba dopustiti vašem serveru da sinhronizuje vreme samo sa odre?enog broja eksternih servera. Zabraniti klijentima da komuniciraju sa NTP serverima na Internetu.

Tre?a varijanta je kada nemate svoj NTP server nego ra?unari iz vaše mreže koriste usluge eksternih NTP servera. Tada treba odabrati eksterne servere i klijentima iz vaše mreže dopustiti da kominiciraju samo sa odabranim serverima.

Preporuke:

- Izbor strategije filtriranja NTP servisa zavisi od institucije/organizacije. Konkretne preporuke ?e biti dopisane za strategiju koju budemo identifikovali kao najšire primenjljivu u AMRESu u toku diskusije o ovom dokumentu.

SNMP

SNMP (Simple Network Management Protocol) je standarni protokol za nadgledanje i upravljanje mrežnim ure?ajima. SNMP arhitektura se sastoji od dva klju?na elementa: agenta i menadžera. Radi se o klijent-server arhitekturi u kojoj je agent server, a menadžer klijent. Agent je program koji se izvršava na nekom nadziranom ?voru mreže. To je u stvari server proces, koji šalje podatke menadžeru i prima upravlja?ke naredbe. Menadžer je program koji se izvršava na stanici za nadzor mreže (klijent proces) i njegova uloga je da kontaktira razne agente i prikuplja podatke od njih. SNMP agent može da šalje poruke i bez prethodnog zahteva od strane menadžera (trap poruke).

Trenutno su u upotrebi dve verzije SNMP protokola, v2 i v3. SNMP v3 ima poboljšane karakteristike sa aspekta bezbednosti.

SNMP koristi UDP kao transportni mehanizam za SNMP poruke, mada može da koristi i TCP. SNMP agenti koriste UDP portove 161 i 162 (za trap). SNMP menadžeri (klijenti) koriste portove iznad 1023 za komunikaciju sa agentima (serverima). Sve verzije SNMP koriste iste brojeve za portove.

Direction	Source addr.	Dest. addr.	Protocol	SourcePort	Dest.port	ACK	Notes
In	Ext	Int	UDP	>1023	161	*	Query from external management station to internal SNMP device
Out	Int	Ext	UDP	161	>1023	*	Response from internal SNMP device to external management station

Out	Int	Ext	UDP	>1023	161	*	Query from internal management station to external SNMP device
In	Ext	Int	UDP	161	>1023	*	Response from external SNMP device to internal management station
In	Ext	Int	UDP	162	>1023	*	Trap from external SNMP device to internal management station
Out	Int	Ext	UDP	>1023	162	*	Trap from internal SNMP device to external management station

* UDP ne koristi ACK fleg

Najbolja zaštita je ako onemogu?ite da neko spolja uzima podatke sa vaših ure?aja odnosno nadgleda vašu mrežu.

Preporuke:

- Poželjno je da TCP i UDP saobra?aj sa svih portova sa Interneta bude blokiran ka vašim internim resursima na portovima 161 i 162.
- Ukoliko je neophodno da upravljate vašim internim resursima sa externih servera, onda koristite SNMPv3.

File Transfer Protocol(FTP)

FTP (File Transfer Protocol) je naj?eš?e koriš?en protokol za prenos podataka izme?u dva ra?unara na mreži. Za svoj rad korist TCP. Autentifikacija i sva komunikacija se prenose kao otvoren tekst što ovaj protokol ?ini ne tako bezbednim.

FTP sesija se sastoji od dve konekcije: kontrolne konekcije i konekcije za prenos podataka. Kontrolna konekcija se pokre?e prva i šalje zahtev za uspostavljanje veze udaljenom ra?unaru. Nakon provere identiteta i uspostavljanja dvosmerne veze, klijent je u mogu?nosti da šalje komande za obavljanje razli?itih zadataka. Kada klijent napravi zahtev za prenos podataka, tada se aktivira konekcija za prenos podataka (na drugom portu) koja vrši sam prenos. Za to vreme kontrolna sesija mora ostati aktivna kako bi se komande i poruke mogle razmenjivati izme?u klijenta i servera.

FTP radi u dva režima i važno je razumeti razliku izme?u ova dva režima zbog firewall pravila.

Aktivni režim

U aktivnom režimu klijent inicira konekciju sa slu?ajno izabranog porta iznad 1023 (N) ka FTP serveru na portu 21. Zatim salje serveru naredbu PORT N+1, gde je N+1 port na kome ?e klijent da prima podatke. Server zatim otvara kanal za prenos podataka sa porta 20 ka portu N+1 na strani

klijenta.

Pasivni rezim

U pasivnom režimu klijent alocira dva porta za sebe (N, N+1) i prvi port (N) koristi da inicira konekciju sa FTP serverom na portu 21. Zatim šalje serveru naredbu PASV što govori serveru da alocira port za prenos podataka (iznad 1023) i šalje klijentu ovaj broj porta. Zatim, klijent otvara konekciju za prenos podataka sa porta (N+1) ka portu za prenos podataka na strani servera.

Direction	Source addr.	Dest. addr.	Protocol	SourcePort	Dest.port	ACK *	Notes
In	Ext	Int	TCP	>1023	21	**	Incoming FTP request, active mode
Out	Int	Ext	TCP	21	>1023	Yes	Response to incoming request, active mode
Out	Int	Ext	TCP	20	>1203	**	Data channel creation for incoming FTP request, active mode
In	Ext	Int	TCP	>1023	20	Yes	Data channel response for incoming FTP request, active mode
In	Ext	Int	TCP	>1023	21	**	Incoming FTP request, passive mode
Out	Int	Ext	TCP	21	>1023	Yes	Response to incoming request, passive mode
In	Ext	Int	TCP	>1023	>1023	**	Data channel creation for incoming FTP request, passive mode
Out	Int	Ext	TCP	>1023	20	Yes	Data channel response for incoming FTP request, passive mode
Out	Int	Ext	TCP	>1023	21	**	Outgoing FTP request, active mode
In	Ext	Int	TCP	21	>1023	Yes	Response to outgoing request, active mode
In	Ext	Int	TCP	20	>1203	**	Data channel creation for outgoing FTP request, active mode
Out	Int	Ext	TCP	>1023	20	Yes	Data channel response for outgoing FTP request, active mode
Out	Int	Ext	TCP	>1023	21	**	Outgoing FTP request, passive mode
In	Ext	Int	TCP	21	>1023	Yes	Response to outgoing request, passive mode
Out	Int	Ext	TCP	>1023	>1203	**	Data channel creation for outgoing FTP request, passive mode

In	Ext	Int	TCP	>1023	>1023	Yes	Data channel response for outgoing FTP request, passive mode

* Ukoliko postoji mogu?nost kontrole ACK flega

** ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

Preporuke:

- Ukoliko imate klijente koji podržavaju pasivni FTP režim, možete da dozvolite sa komuniciraju sa eksternim serverima preko firewall-a.
- Ukoliko imate FTP klijente koji ne podržavaju pasivni režim onda je najbolje da koristite proksi server koji ima TIS Firewall Toolkit.
- Razmotrite pružanje FTP servisa omogu?avanjem oba na?ina: pasivni mod preko firewall-a i aktivni mod preko proksija.
- Ukoliko želite da omogu?ite dolazne FTP konekcije, omogu?ite to preko firewall-a samo do unapred definisanih FTP servera.

NetBIOS, RPC, SMB/CIFS over TCP/IP

Razmotri?emo još nekoliko servisa koji su od zna?aja za bezbednost ra?unara unutar mreže:

- NetBIOS (Network Basic Input/Output Sistem) je program koji omogu?ava ra?unarima da komuniciraju u okviru lokalne mreže. On je deo NetBEUI interfejsa u okviru Windows operativnog sistema. On sam ne podržava rutiranje u okviru WAN mreža ali može da koristi druge transportne mehanizme kao što je TCP. NetBIOS pruža tri razli?ite usluge:
  - Name service, se koristi za identifikaciju resursa na mreži, koristi UDP/TCP port 137
  - Session service, NetBIOS sesije izme?u ra?unara u cilju prenosa podataka, koristi TCP/UDP 139.
  - Datagram service, slanje datagrama jednom ra?unaru ili svim ?lanovima LAN-a, koristi UDP 138.

- RPC (Remote procedure Call) je protokol koji omogu?ava da program na jednom ra?unaru pokrene program na drugom ra?unaru (serveru). To je klasi?na klijent-server arhitektura. Standardno, na Windows serverima ovaj servis koristi TCP/UDP port 135.

- SMB (Server Message Block) je protokol za deljenje štampa?a i fajlova izme?u ra?unara na mreži. SMB je originalno dizajniran da radi na NetBIOS protokolu ali je kasnije dobio podršku za TCP/IP. CIFS (Common Internet File System) predstavlja noviju verziju SMB-a koja nudi odre?ena poboljšanja i radi na TCP/IP umesto NetBIOS protokolu. SMB/CIFS koriste TCP/UDP port 445 ako idu direktno preko TCP/IP odnosno TCP 139 i UDP 138 ako idu preko preko NetBIOS over TCP/IP.

Pored toga što generišu dodatni saobra?aj u mreži, kod ovih servisa, u prošlosti, otkriveni su brojni bezbednosni propusti koji su uzrokovali pove?anu ranjivost ra?unara u mreži.

Preporuke:

- Ove servise treba pustiti da budu aktivni u okviru LAN-a, a dolazni i odlazni saobra?aj za portove 135, 137-139 i 445, TCP i UDP onemogu?iti izvan lokalne mreže.

IP Spoofing

IP spoofing je tehnika napada kada napada? zamenjuje (lažira) izvorišnu ili odredišnu IP adressu paketa.

U slu?aju falsifikovanja adrese izvora paketa, paket se pojavljuje kao da je poslat sa druge adrese ili sa više razli?itih adresa. Ra?unar koji prima pakete svoje odgovore šalje na falsifikovane adrese. U odre?enim slu?ajevima je mogu?e da napada? preusmeri odgovor na svoj ra?unar.

Ova tehnika se koristi u cilju izvo?ena razli?itih vrsta napada na ure?aje u okviru jedne mreže. Filtriranje paketa je jedan od na?ina za odbranu od IP Spoofinga.

Preporuke:

- Blokirai sve dolazne IP pakete sa *source* adresom iz adresnog prostor vaše mreže.
- Blokirati odlazne IP paketa generisane u internoj mreži sa *source* adresom koja ne pripadaju vašoj mreži. Ukoliko mrežni ure?aji imaju uRPF (Unicast Reverse Path Forwarding) svakako treba koristiti ovu opciju za blokiranje lažnih adresa iz vaše mreže.
- Posebnu pažnju posvetiti filtriranju privatnih adresa iz vaše mreže.

VPN

Pravila o filtriranju saobra?aja moraju podržavi razli?ite scenarije korištenja VPN tehnologije.

Dva naj?eš?a modela implementacije VPN arhitekture su gateway-to-gateway i host-to-gateway.

Gateway-to-gateway

Gateway-to-gateway model omogu?ava povezivanje dve mreže, preko njihovih *gateway* ure?aja koji me?usobno uspostavljaju VPN konekciju. *Gateway* ure?aj može biti *firewall* ure?aj, VPN server ili ruter. VPN konekcija pruža zaštitu komunikaciji izme?u hostova, u ove dve, razli?ite mreže, ali samo u delu izme?u *gateway* ure?aja. Komunikacija izme?u *host*a i njegovog *gateway* ure?aja nije zašti?ena. Ovakav tip arhitekture se naj?eš?e primenjuje u povezivanju udaljenih i obezbe?enih mreža preko Interneta. *Gateway-to-gateway* model rada je transparentan za krajnje *host*ove i **ne zahteva** instalaciju ili konfiguraciju dodatnog softvera na krajnjim ra?unarima da bi ostvarili komunikaciju.

Host-to-gateway

Host-to-gateway model omogu?ava povezivanje hostova iz udaljenih mreža sa hostovima unutar neke organizacije, primenom VPN gateway ure?aja (npr. firewall ure?aj, VPN server ili ruter). Hostovi iz udaljenih mreža, uspostavljaju individualne VPN konekcije sa gateway ure?ajem. Na ovaj na?in, VPN konekcija pruža zaštitu komunikaciji izme?u udaljenog hosta i gateway ure?aja, ali ne i izme?u gateway ure?aja i odredišnog hosta, koji se nalaze u mreži te organizacije. Naj?eš?a primena ovog modela, jeste u povezivanju hostova iz neobezbe?enih mreža sa resursima i hostovima u obezbe?enim mrežama (npr. povezivanje zaposlenih od ku?e, iz hotela ili aerodroma) na mrežu institucije preko Internet infrastrukture. Host-to-gateway model rada nije transparentan za krajnje korisnike, jer zahteva da se svaki korisnik autentifikuje pre uspostavljanja VPN konekcije, a tako?e zahtevaju i instalaciju i konfiguraciju VPN klijent softvera na korisni?kim ure?ajima.

Na osnovu dokumenta AMRES 2008 – “D02. Realizacija VPN servisa za AMRES pojedina?ne korisnike”, možemo izdvojiti slede?a VPN rešenja, kao preporuke za realizaciju u okviru AMRES mreže:

1. Host-to-gateway arhitektura – PPTP, L2TP/IPSec, SSL VPN
2. Gateway-to-gateway arhitektura – PPTP, GRE/IPSec

SSL VPN

Secure Socets Layer (SSL) VPN omogu?ava bezbedan na?in pristupa udaljenim reursima neke mreže. Saobra?aj izme?u SSL klijenta i SSL servera je enkriptovan pomo?u SSL/TLS protokola.

Da bi se omogu?ilo nesmetano funkcionisanje SSL VPN servisa, potrebno je omogu?iti komunikaciju ka VPN gateway ure?aju po TCP portu 443.

Direction	Source IP address	Destination IP address	Protocol	Source port	Destination port	Notes
In	Ext	Int	TCP	>1023	443	Komunikacija eksternih klijenta ka internom VPN serveru
Out	Int	Ext	TCP	443	>1023	Komunikacija internog VPN servera ka eksternim klijentima
Out	Int	Ext	TCP	>1023	443	Komunikacija internih klijenta ka eksternom VPN serveru
In	Ext	Int	TCP	443	>1023	Komunikacija eksternog VPN servera ka internim klijentima

PPTP

PPTP (Point-to-point Tunneling Protocol) osigurava komunikaciju izme?u PPTP klijenta i PPTP servera i koristi GRE protokol za transport podataka izme?u njih. Protokoli i TCP/UDP portovi neophodni za funkcionisanje ovg servisa su predstavljeni u tabeli ispod.

Direction	Source IP address	Destination IP address	Protocol	Source port	Destination port	Notes
In	Ext	Int	TCP	>1023	1723	This filter allows PPTP tunnel maintenance traffic from the external PPTP client to the internal PPTP server.
In	Ext	Int	GRE	-	-	This filter allows PPTP tunneled data from the external PPTP client to the internal PPTP server.
Out	Int	Ext	TCP	1723	>1023	This filter allows PPTP tunnel maintenance traffic from the internal VPN server to the external VPN client.
Out	Int	Ext	GRE	-	-	This filter allows PPTP tunneled data from the internal VPN server to the external VPN client.
Out	Int	Ext	TCP	>1023	1723	This filter allows PPTP tunnel maintenance traffic from the internal PPTP client to the external PPTP server.
Out	Int	Ext	GRE	-	-	This filter allows PPTP tunneled data from the internal PPTP client to the external PPTP server.
In	Ext	Int	TCP	1723	>1023	This filter allows PPTP tunnel maintenance traffic from the external VPN server to the internal VPN client.
In	Ext	Int	GRE	-	-	This filter allows PPTP tunneled data from the external VPN server to the internal VPN client.

L2TP/IPSec

L2TP (Layer 2 Transport Protocol) je jedan od enkapsulacionih protokola, koji se koristi za formiranje tunela u IP mrežama. Ovaj protokol ne enkriptuje poruku koju prenosi. Zbog te svoje osobine, u IP mrežama se naj?eš?e koristi u kombinaciji sa IPSec protokol stekom koji pruža mehanizme enkripcije. TCP/UDP portovi i odgovaraju?i protokoli potrebni za funkcionisanje L2TP/IPSec VPN servisa su prikazani u tabeli ispod.

Direction	Source IP address	Destination IP address	Protocol	Source port	Destination port	Notes

In	Ext	Int	UDP	>1023	500	This filter allows IKE traffic to the internal VPN server.
In	Ext	Int	UDP	>1024	4500	This filter allows IPSec NAT-T traffic to the internal VPN server.
In	Ext	Int	ESP	-	-	This filter allows IPSec ESP traffic from the VPN client to the VPN server.
In	Ext	Int	AH	-	-	This filter allows IPSec AH traffic from the VPN client to the VPN server.
Out	Int	Ext	UDP	500	>1023	This filter allows IKE traffic to the external VPN server.
Out	Int	Ext	UDP	4500	>1023	This filter allows IPSec NAT-T traffic to the external VPN server.
Out	Int	Ext	ESP	-	-	This filter allows IPSec ESP traffic from the internal VPN client to the external VPN server.
Out	Int	Ext	AH	-	-	This filter allows IPSec AH traffic from the internal VPN client to the external VPN server.

Za svoje funkcionisanje, L2TP protokol koristi UDP port 1701. Prilikom prolaska kroz firewall ure?aj, sav L2TP saobra?aj je enkriptovan i enkapsuliran u ESP protokol. Zbog toga, na samom firewall ure?aju nije neophodno otvoriti UDP port 1701, da bi L2TP/IPSec VPN servis funkcionisao.

U tabeli ispod su predstavljene generalne preporuke, za dopuštanje TCP/UDP servisa i odgovaraju?ih protokola, kroz firewall ure?aje, koje treba da obezbede normalno funkcionisanje VPN servisa.

VPN Protokol	**IP protokoli**
IPSec	50 (Authentication Header, for AH connections) 51 (for Encapsulating Security Payload, for ESP connections) 17 (UDP), port 500 (for Internet Key Exchange, whether or not NAT-Traversal is used) 17 (UDP), port 4500 (for Internet Key Exchange using NAT-Traversal)
PPTP	47 (GRE - Generic Routing Encapsulation) 6 (TCP), port 1723
L2TP	17 (UDP), port 1701
SSL/TLS	6 (TCP), port 443
GRE	47 (GRE - Generic Routing Encapsulation)

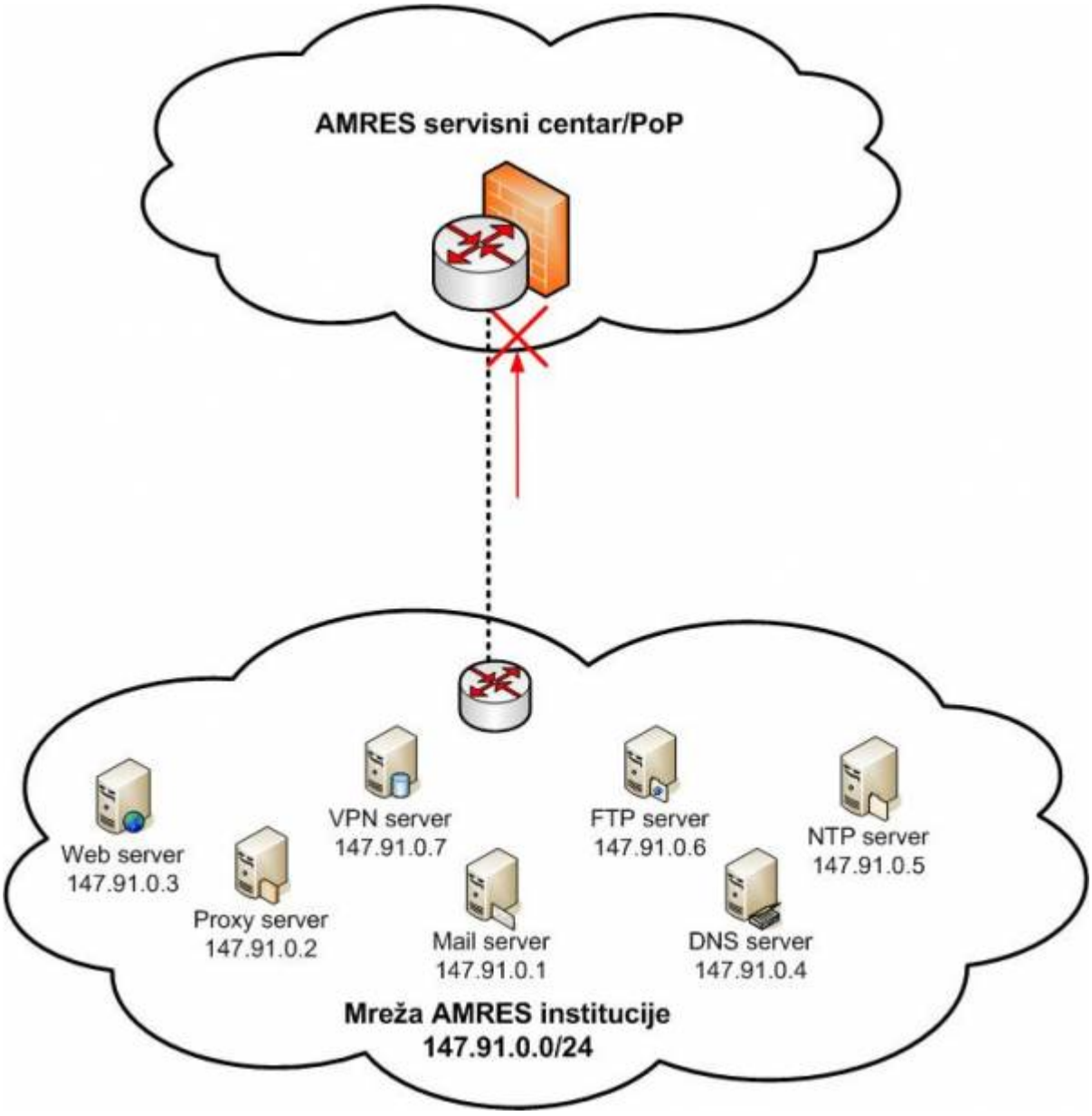
Primeri konfiguracija za liste pristupa (ACL -

access control lists)

Ve?ina institucija u AMRES-u koristi Cisco mrežne ure?aje na poziciji tri. Zbog toga su, u nastavku ovog poglavlja, prikazani primeri konfiguracija ACL, koriš?enjem IOS komandi.

Primer liste pristupa (ACL) za AMRES servisne centre

Ovo je predlog liste pristupa, koja bi se primenila na mrežnom ure?aju u AMRES servisnom centaru/PoP-u. Lista je konfigurisana po tekstu “Pravilnika o filtriranju saobra?aja u AMRES-u”, koji se odnosi na fitriranje saobra?aja na internim vezama. Lista se može primeniti na interfejsu, preko koga je povezana institucija/organizacija ?lanica AMRES-a.



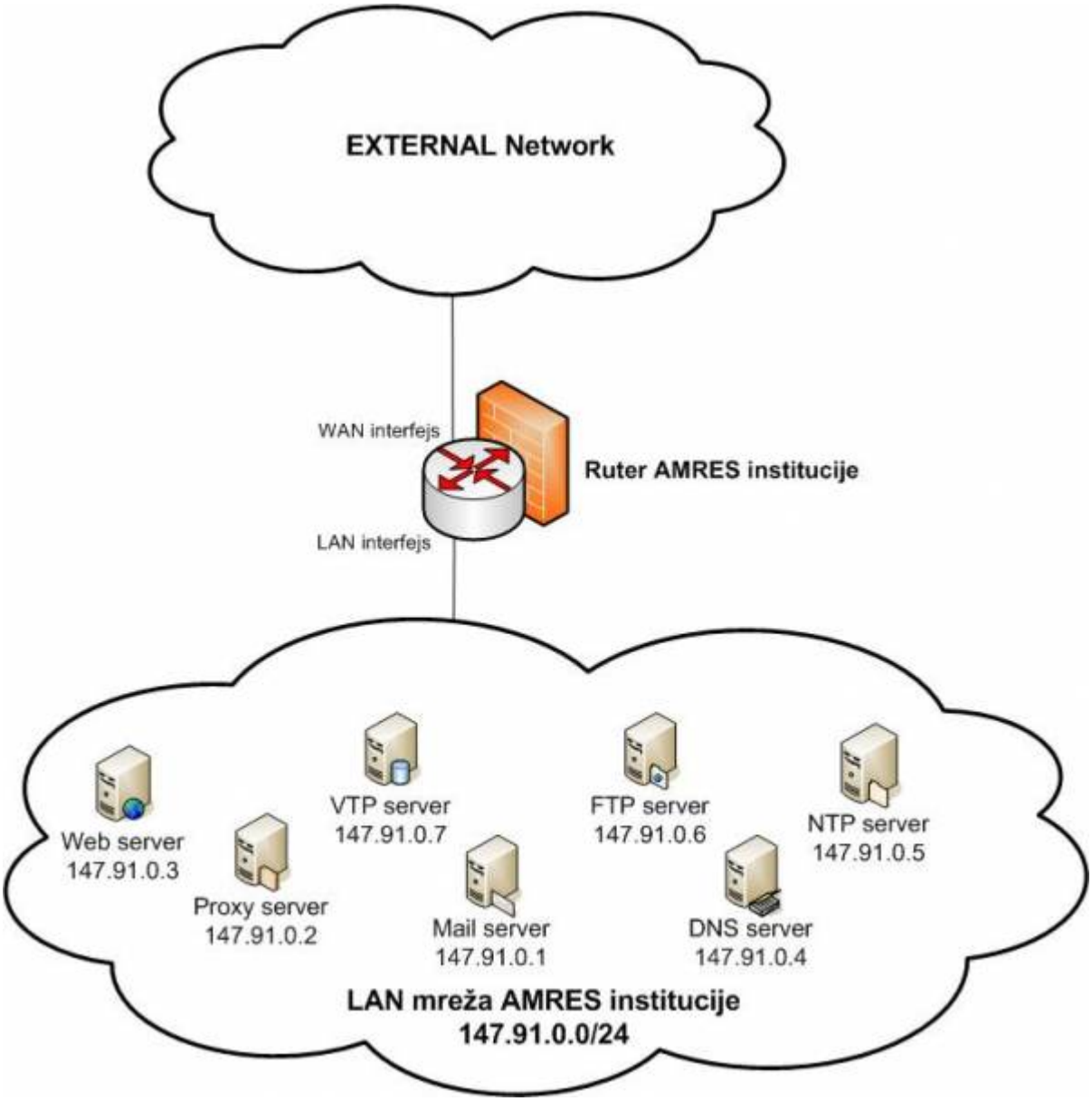

```
! ======================================================
```

```
!
! ACCESS-LIST SITE_in
! za dolazni saobracaj sa udaljene lokacije
! na Akademsku mrezu
!
! ============================================================
no ip access-list extended SITE_in
ip access-list extended SITE_in

! ************************************************************
! GENERALNE ZABRANE
! ************************************************************
!
!------------------------------------------------------------
!   Antispoofing
!------------------------------------------------------------
!
deny ip 10.0.0.0    0.255.255.255   any
deny ip 172.16.0.0  0.31.255.255    any
deny ip 192.168.0.0 0.0.255.255     any
deny ip 127.0.0.0   0.255.255.255   any
deny ip 0.0.0.0     0.255.255.255   any
deny ip 224.0.0.0   31.255.255.255  any
!
!------------------------------------------------------------
!   Protokoli u LAN mrezama
!------------------------------------------------------------
!
deny tcp any range 135 139 any
deny udp any range 135 139 any
deny tcp any any range 135 139
deny udp any any range 135 139
!
deny tcp any eq 445 any
deny udp any eq 445 any
deny tcp any any eq 445
deny udp any any eq 445
!
deny tcp any eq 1434 any
deny udp any eq 1434 any
deny tcp any any eq 1434
deny udp any any eq 1434
!
! ************************************************************
! KONTROLISANI SERVISI
! ************************************************************
!
!------------------------------------------------------------
!    SNMP
!------------------------------------------------------------
!
```

```
permit udp any eq 161 host 147.91.3.12! ICmyNet.IS server
deny udp any eq 161 any
!
permit udp any host 147.91.3.12 eq 162! ICmyNet.IS server
deny udp any any eq 162
!
!-------------------------------------------------------
!    SMTP
!-------------------------------------------------------
permit tcp host 147.91.0.1 any eq 25
permit tcp host 147.91.0.1 eq 25 any
!
permit tcp 147.91.0.0 0.0.0.255 host 147.91.1.120 eq 25 ! slanje poste ka
RCUB Afrodita e-mail serveru
permit tcp 147.91.0.0 0.0.0.255 host 147.91.1.119 eq 25 ! slanje poste ka
RCUB Tesla e-mail serveru
!
deny tcp any any eq 25
deny tcp any eq 25 any
!
!-------------------------------------------------------
!    ICMP
!-------------------------------------------------------
permit icmp host x.x.x.x any echo
permit icmp any 147.91.4.0 255.255.255.0 echo-reply
deny icmp any any
!
! *******************************************************
! Antispoofing
! *******************************************************
permit ip 147.91.0.0 0.0.0.255 any
deny ip any any
!-------------------------------------------------------
```

Primer ACL za institucije ?lanice AMRES-a



U ovom poglavlju su dati primeri komandi za konfiguraciju ACL na Cisco ruterima. Konfiguracija ACL je bazirana na preporukama datim u okviru poglavlja ” Najcesce korisceni servisi”. Za svaki servis je dat primer filtriranja u izlaznom (egress) i ulaznom (ingress) smeru.

U tekstu ispod je dat primer ACL, koja filtrira saobracaj u smeru od lokalne mreže neke AMRES institucije, prema eksternim mrežama (egress traffic filtar). Data ACL je zasnovana na strategiji filtriranja dozvoli sve tj. sav saobra?aj koji nije eksplicitno zabranjen se dopušta. ACL je zasnovana na odgovaraju?im pretpostavkama, koje se ti?u koriš?enja pojedinih servisa od strane AMRES institucije(npr. koristi se eksterni proxy server, lokalni NTP server se sinhroniše sa eksternim NTP serverima, koristi se aktivni mod rada FTP-a, koristi se PPTP VPN servis itd.). Navedena ACL je samo jedan od primera implementacije filtriranja saobra?aja u odlaznom (egress) smeru.

Napomena: U primeru ACL se za IP adresni opseg LAN mreže AMRES institucije, koristi opseg 147.91.0.0/24. Sve IP adrese eksternih hostova su ozna?ene kao x.x.x.x.

!

```
------------------------------------------------------------------------------
--------------------
!
! ACCESS-LIST INSTITUCIJA_out
! filtriranje saobracaja u smeru od LAN mreze institucije prema eksternim
mrežama
!
!
------------------------------------------------------------------------------
---------------------
!
no ip access-list extended INSTITUCIJA_out
ip access-list extended INSTITUCIJA _out
!
!-----------------------------------------------------------------------------
----------------------
! E-mail servis
!-----------------------------------------------------------------------------
----------------------
!
!---- SMTP ----
!
permit tcp host 147.91.0.1 gt 1023 any eq 25
permit tcp host 147.91.0.1 eq 25 any gt 1023
!
permit tcp any gt 1023 host x.x.x.x eq 25 ! slanje pošte ka identifikovanim,
eksternim e-mail serverima
!
deny tcp any gt 1023 any eq 25 ! zabrana slanja pošte sa klijenata koji nisu
identifikovani kao e-mail serveri
!
deny tcp any eq 25 any gt 1023! zabrana slanja pošte sa klijenata koji nisu
identifikovani kao e-mail serveri
!
!
!---- POP3/POP3S ----
!
permit tcp any gt 1023 host x.x.x.x eq 995 ! primanje pošte sa
identifikovanih, eksternih e-mail servera
!
deny tcp any gt 1023 any eq 995
deny tcp any gt 1023 any eq 110
!
permit tcp host 147.90.0.1 eq 995 any gt 1023 ! slanje pošte ka eksternim
klijentima
!
deny tcp any eq 995 any gt 1023 ! zabrana slanja pošte sa klijenata koji nisu
identifikovani kao e-mail serveri
deny tcp any eq 110 any gt 1023 ! zabrana slanja pošte sa klijenata koji nisu
identifikovani kao e-mail serveri
!
```

```
!---- IMAP/IMAPS ----
!
permit tcp any gt 1023 host x.x.x.x  eq 993 ! primanje pošte sa
identifikovanih, eksternih e-mail servera
!
deny tcp any gt 1023 any eq 993
deny tcp any gt 1023 any eq 143
!
permit tcp host 147.90.0.1 eq 993 any gt 1023 ! slanje pošte ka eksternim
klijentima
!
deny tcp any eq 993 any gt 1023 ! zabrana slanja pošte sa klijenata koji nisu
identifikovani kao e-mail serveri
deny tcp any eq 143 any gt 1023 ! zabrana slanja pošte sa klijenata koji nisu
identifikovani kao e-mail serveri
!
!-------------------------------------------------------------------------
-----------------------
! WEB servis
!-------------------------------------------------------------------------
-----------------------
!
!---- HTTP/HTTPS ----
!
! AMRES institucija koristi eksterni proxy server
!
permit tcp any gt 1023 host x.x.x.x eq 8080
deny tcp any gt 1023 any eq 80
deny tcp any gt 1023 any eq 443
deny tcp any gt 1023 any eq 8080
!
! AMRES institucija poseduje lokalni WEB server
!
permit tcp host 147.91.0.3 eq 80 any gt 1023
permit tcp host 147.91.0.3 eq 443 any gt 1023
deny tcp any eq 80 any gt 1023
!
!-------------------------------------------------------------------------
-----------------------
! DNS servis
!-------------------------------------------------------------------------
-----------------------
!
!---- DNS ----
!
permit tcp any gt 1023 any eq 53 ! upiti na eksterne DNS servere
permit udp any gt 1023 any eq 53
!
permit tcp host 147.91.0.4 eq 53 any gt 1023 ! odgovor lokalnog DNS servera
na eksterne upite, transfer zonske tabele ka eksternim DNS serverima
permit udp host 147.91.0.4 eq 53 any gt 1023
```

```
!
permit udp host 147.91.0.4 eq 53 any eq 53 ! komunikacija internog sa
eksternim DNS serverima
!
deny tcp any eq 53 any gt 1023
deny udp any eq 53 any gt 1023
deny udp any eq 53 any eq 53
!
!-------------------------------------------------------------------------
-----------------------
! Remote Access servis
!-------------------------------------------------------------------------
-----------------------
!
!---- Telnet ----
!
permit tcp any gt 1023 any eq 23
permit tcp host 147.91.0.5 eq 23 host x.x.x.x gt 1023
deny tcp any eq 23 any gt 1023
!
!---- SSH ----
!
permit tcp any any eq 22
permit tcp host 147.91.0.5 eq 22 any
deny tcp any eq 22 any
!
!-------------------------------------------------------------------------
-----------------------
! VPN servis
!-------------------------------------------------------------------------
-----------------------
!
!---- PPTP VPN ----
!
permit gre any any
permit tcp any gt 1023 host x.x.x.x eq 1723
!
permit tcp host 147.91.0.7 eq 1723 any gt 1023
!
deny tcp any gt 1023 any eq 1723
deny tcp any eq 1723 any gt 1023
!
!-------------------------------------------------------------------------
-----------------------
! Ostali servisi
!-------------------------------------------------------------------------
-----------------------
!
!---- Ping ----
!
permit icmp any any echo
```

```
permit icmp any 147.91.4.0 255.255.255.0 echo-reply! primer administratorske
mreže ka kojoj su dozvoljeni icmp echo-reply odgovori
deny icmp any any echo-reply
!
!---- NTP ---- (pretpostavka da nema klijenata sa eksternih mreža koje se
sinhronišu sa lokalnim NTP serverom)
!
! lokalni NTP server sa sinhronizacijom na Internetu
!
permit udp host 147.91.0.5 eq 123 host x.x.x.x eq 123
deny udp any gt 1023 any eq 123
deny udp any eq 123 any gt 1023
deny udp any eq 123 any eq 123
!
!---- SNMP ----
!
deny udp any eq 161 any gt 1023
deny udp any eq 162 any gt 1023
!
!---- FTP (aktivni mod) ----
!
permit tcp any gt 1023 any eq 21
permit tcp any gt 1023 any eq 20
!
permit tcp host 147.91.0.6 eq 21 any gt 1023
permit tcp host 147.91.0.6 eq 20 any gt 1023
!
deny tcp any eq 21 any gt 1023
deny tcp any eq 20 any gt 1023
!
!---- NetBIOS, RPC, SMB/CIFS ----
!
deny tcp any any range 135 139
deny udp any any range 135 139
!
deny tcp any range 135 139 any
deny udp any range 135 139 any
!
deny tcp any any eq 445
deny udp any any eq 445
!
deny tcp any eq 445 any
deny udp any eq 445 any
!
!-------------------------------------------------------------------------
-----------------------
! Antispoofing
!-------------------------------------------------------------------------
-----------------------
!
permit ip 147.91.0.0 0.0.0.255 any
```

```
deny ip any any
!
!-------------------------------------------------------------------------
----------------------
```

U tekstu ispod je dat primer ACL, koja filtrira saobracaj u smeru od eksternih mreža, prema lokalnoj mreži AMRES institucije (ingress traffic filtar). Data ACL je zasnovana na strategiji filtriranja dozvoli sve tj. sav saobra?aj koji nije eksplicitno zabranjen se dopušta. ACL je zasnovana na odgovaraju?im pretpostavkama, koje se ti?u koriš?enja pojedinih servisa od strane AMRES institucije(npr. koristi se eksterni proxy server, lokalni NTP server se sinhroniše sa eksternim NTP serverima, koristi se aktivni mod rada FTP-a, koristi se PPTP VPN servis itd.). Navedena ACL je samo jedan od primera implementacije filtriranja saobra?aja u dolaznom (ingress) smeru.

Napomena: U primeru ACL se za IP adresni opseg LAN mreže AMRES institucije, koristi opseg 147.91.0.0/24. Sve IP adrese eksternih hostova su ozna?ene kao x.x.x.x.

```
!
----------------------------------------------------------------------------
---------------------
!
! ACCESS-LIST INSTITUCIJA_in
! filtriranje saobracaja u smeru od eksternih mreža prema lokalnoj mreži
AMRES institucije
!
!
----------------------------------------------------------------------------
---------------------
!
 no ip access-list extended INSTITUCIJA_in
 ip access-list extended INSTITUCIJA _in
!
!-------------------------------------------------------------------------
-----------------------
! E-mail servis
!-------------------------------------------------------------------------
-----------------------
!
!---- SMTP ----
!
permit tcp any eq 25 host 147.91.0.1 gt 1023 ! odlazni mail
permit tcp any gt 1023 host 147.91.0.1 eq 25 ! dolazni mail
!
permit tcp host x.x.x.x eq 25 any gt 1023 ! u slucaju externih mail servera
!
deny tcp any eq 25 any gt 1023 ! dolazni mail saobra?aj (prijem pošte) samo
na te servere.
deny tcp any gt 1023 any eq 25 ! dolazni mail saobra?aj (prijem pošte) samo
na te servere.
!
```

```
!---- POP3/POP3S ----
!
permit tcp host x.x.x.x eq 995 any gt 1023
!
deny tcp any eq 995 any gt 1023
deny tcp any eq 110 any gt 1023
!
permit tcp any gt 1023 host 147.91.0.1 eq 995
!
deny tcp any gt 1023 any eq 995
deny tcp any gt 1023 any eq 110
!
!---- IMAP/IMAPS ----
!
permit tcp host x.x.x.x eq 993 any gt 1023
!
deny tcp any eq 993 any gt 1023
deny tcp any eq 143 any gt 1023
!
permit tcp any gt 1023 host 147.91.0.1 eq 995
!
deny tcp any gt 1023 any eq 993
deny tcp any gt 1023 any eq 143
!
!-------------------------------------------------------------------------------
-----------------------
! WEB servis
!-------------------------------------------------------------------------------
-----------------------
!
!---- HTTP/HTTPS ----
!
! AMRES institucija koristi eksterni proxy server
!
permit tcp host x.x.x.x eq 8080 any eq 1023
deny tcp any eq 80 any gt 1023
deny tcp any eq 443 any gt 1023
deny tcp any eq 8080 any gt 1023
!
! AMRES institucija poseduje lokalni WEB server
!
permit tcp any gt 1023 host 147.91.0.3 eq 80
permit tcp any gt 1023 host 147.91.0.3 eq 443
deny tcp any gt 1023 any eq 80
deny tcp any gt 1023 any eq 443
!
!-------------------------------------------------------------------------------
-----------------------
! DNS servis
!-------------------------------------------------------------------------------
-----------------------
```

```
!
!---- DNS ----
!
permit tcp any gt 1023 host 147.91.0.4 eq 53
permit udp any gt 1023 host 147.91.0.4 eq 53
!
permit tcp any eq 53 any gt 1023
permit udp any eq 53 any gt 1023
!
permit udp any eq 53 host 147.91.0.4 eq 53
!
deny tcp any gt 1023 any eq 53
deny udp any gt 1023 any eq 53
deny udp any eq 53 any eq 53
!
!-------------------------------------------------------------------------
------------------------
! Remote Access servis
!-------------------------------------------------------------------------
------------------------
!
!---- Telnet ----
!
permit tcp any eq 23 any gt 1023
permit tcp host x.x.x.x gt 1023 host 147.91.0.5 eq 23
deny tcp any gt 1023 any eq 23
!
!---- SSH ----
!
permit tcp any eq 22 any
permit tcp any host 147.91.0.5 eq 22
deny tcp any any eq 22
!
!-------------------------------------------------------------------------
------------------------
! VPN servis
!-------------------------------------------------------------------------
------------------------
!
!---- PPTP VPN ----
!
permit gre any any
permit tcp host x.x.x.x eq 1723 any gt 1023
!
permit tcp any gt 1023 host 147.91.0.7 eq 1723
!
deny tcp any eq 1723 any gt 1023
deny tcp any gt 1023 any eq 1723
!
!-------------------------------------------------------------------------
------------------------
```

```
! Ostali servisi
!-------------------------------------------------------------------------
-----------------------
!
!---- Ping ----
!
permit icmp any any eq echo-reply
permit icmp 147.91.4.0 255.255.255.0 any echo
deny icmp any any echo
!
!---- NTP ---- (pretpostavka da nema klijenata sa eksternih mreža koje se
sinhronišu sa lokalnim NTP serverom)
!
! lokalni NTP server sa sinhronizacijom na Internetu
!
permit udp host x.x.x.x eq 123 host 147.91.0.5 eq 123
deny utp any gt 1023 any eq 123
deny utp any eq 123 any gt 1023
deny utp any eq 23 any eq 23
!
!
!---- SNMP ----
!
deny udp any gt 1023 any eq 161
deny udp any gt 1023 any eq 162
!
!---- FTP (aktivni mod) ----
!
permit tcp any gt 1023 host 147.91.0.6 eq 21
permit tcp any gt 1023 host 147.91.0.6 eq 20
!
permit tcp any eq 21 any gt 1023
permit tcp any eq 20 any gt 1023
!
deny tcp any gt 1023 any eq 21
deny tcp any gt 1023 any eq 20
!
!---- NetBIOS, RPC, SMB/CIFS ----
!
deny tcp any any range 135 139
deny udp any any range 135 139
!
deny tcp any range 135 139 any
deny udp any range 135 139 any
!
deny tcp any any eq 445
deny udp any any eq 445
!
deny tcp any eq 445 any
deny udp any eq 445 any
!
```

```
!------------------------------------------------------------------------------
----------------------
! Antispoofing
!------------------------------------------------------------------------------
----------------------
!
permit ip any 147.91.0.0 0.0.0.255
deny ip any any
!
!------------------------------------------------------------------------------
----------------------
```

Dodatak : Filtriranje saobra?aja po OSI i TCP/IP slojevima

Pravila filtriranja se po pravilu definišu imaju?i u vidu protokole transportnog (TCP, UDP) i/ili mrežnog sloja (IP, ICMP). Radi kompletnosti, u ovom poglavlju ?e biti pomenuti i osnovni razlozi filtriranja saobra?aja na aplikativnom sloju i sloju prenosa podataka (data link layer).

Aplikativni sloj

Aplikativni sloj je najviši sloj u hijararhiji TCP/IP referentnog modela. On predstavlja interfejs izme?u aplikacija koje koristimo pri komunikaciji i mrežnih resursa koji omogu?avaju prenos korisni?kih poruka. Njegova glavna uloga je da pripremi poruke, svojstvene me?uljudskoj komunikaciji, za prenos preko mreže.

Protokoli, razvijeni na ovom sloju, su zaduženi za razmenu podataka izme?u pokrenutih programa na izvorišnom i odredišnom hostu. Primer protokola aplikativnog sloja su HTTP, SMTP, DNS, FTP itd.

Unutar aplikativnog sloja mogu se na?i i dodatni slojevi protokola. Primer je SMTP protokol koji koristi RFC 2822 sintaksu poruke, da bi mogla da se ubaci ekstenzija MIME (Multipurpose Internet Mail Extensions), koja dalje omogu?ava koriš?enje razli?itih formata poruke (npr. HTML). Ti dublji slojevi protokola, mogu se filtrirati samo na aplikativnom sloju.

Filtriranje poruka aplikativnog sloja, je najsloženiji vid filtriranja saobra?aja u mrežama. Ono se može vršiti na osnovu redosleda razmenjenih poruka odre?enog protokola ili ?ak na osnovu sadržaja samih poruka koje se prenose. Zbog toga, filtriranje saobra?aja na ovom sloju, pruža i najviši stepen zaštite nekoj mreži.

Transportni sloj

Transportni sloj je odgovoran za prenos poruka aplikativnog sloja sa-kraja-na-kraj mreže. Funkcionalnosti implementirane na ovom sloju omogu?avaju, da više aplikacija, pokrenutih na istom ure?aju, vrše istovremenu komunikaciju kroz mrežu. Tako?e, ovaj sloj omogu?ava i pozdan prenos poruka koje se prenose, a pruža i odgovaraju?e mehanizme za detekciju grešaka, koje se mogu javiti

pri prenosu.

Da bi bio u mogu?nosti, da podatke koje prenosi, i prosledi pravoj aplikaciji, transportni sloj mora identifikovati destinacionu aplikaciju. Zbog toga, transportni sloj svakoj aplikaciji dodeljuje i odgovaraju?i identifikator, koji se još naziva i broj porta. Portovi pružaju mehanizam za efikasno filtriranje pojedinih servisa.

Zbog razli?itih zahteve i potreba koje imaju razli?ite aplikacije, razvijeno je nekoliko protokola transportnog sloja. Najzna?ajniji protokoli su TCP (Transmission Control Protocol) i UDP (User Datagram Protocol).

TCP (Transmission Control Protocol) je zasnovan na procesu uspostavljanja konekcije izme?u krajnjih hostova u komunikaciji. Jedna od najbitnijih njegovih uloga je da obezbedi pouzdan prenos podataka u IP okruženju.

UDP (User Datagram Protocol) je jednostavniji protokol u odnosu na TCP, ali i pruža dosta uži skup funkcionalnosti u odnosu na njega. Koristi se za aplikacije kojima je važna brzina prenosa paketa (DNS, Video Streaming, VoIP itd.)

Koriš?enjem odgovaraju?ih brojeva portova, mogu?e je dozvoliti ili zabraniti tok podataka nekog protokola aplikativnog sloja, kroz mrežu. Filtriranjem saobra?aja na ovom sloju, može se efikasno pove?ati nivo bezbednosti neke mreže.

Mrežni sloj

Za razliku od transportnog sloja , ?ija je uloga da omogu?i prenos podataka izme?u krajnjih aplikacija, mrežni sloj je zadužen za obezbe?ivanje komunikacije izme?u krajnjih hostova. Njegova uloga je da pruži servis razmene paketa kroz mrežu identifikovanim, krajnjim ure?ajima. Da bi pružio ovaj servis, mrežni sloj koristi mehanizme adresiranja i rutiranja paketa kroz mrežu. Najzna?ajniji protokoli ovoga sloja su IP (Internet Protocol) i ICMP (Internet Control Message Protocol).

IP (Internet Protocol) je najrasprostranjeniji protokol mrežnog sloja na Internetu. On pruža samo osnovne funkcionalnosti, koje su neophodne za slanje paketa od izvorišnog do odredišnog ure?aja u mreži. Osnovne karakteristike IPv4 protokola su da nema uspostavljanja konekcije izme?u krajnjih hostova u komunikaciji, ovaj protokol, kao i UDP, ne pruža servis pouzdanog prenosa i nezavisan je od medijuma preko koga se odvija komunikacija.

Da bi mogli uspešno da komuniciraju, milioni razli?itih hostova na Internetu moraju biti jedinstveno identifikovani. Servis identifikacije ure?aja na Internetu (adresiranje) pruža upravo IP protokol, preko IP adresa koje se nalaze u zaglavlju svakog paketa. U zaglavlju svakog paketa se nalazi IP adresa izvorišnog hosta (hosta koji šalje paket) i IP adresa odredišnog hosta (hosta koji prima poslati paket).

Pored adresiranja, IP protokol omogu?ava i rutiranje paketa na Internetu. Proces rutiranja

podrazumeva pronalaženje putanje kroz mrežu do odredišnog ure?aja. Rutiranje se obavlja na osnovu informacija o dostupnim mrežama, a koje se dobijaju preko razli?itih ruting protokola (BGP, OSPF, IS-IS, EIGRP itd.). Na osnovu odredišne IP adrese u paketu i informacija o dostupnim mrežama smeštenim u ruting tabeli, mrežni ure?aji obavljaju funkciju rutiranja u mrežama.

Iako, IP protokol ne pruža servis pouzdanog prenosa, on omogu?ava slanje poruka o odgovaraju?im vrstama problema koji se javljaju pri prenosu. Ove poruke se šalju zahvaljuju?i ICMP (Internet Control Message Protocol) protokolu.

ICMP protokol je protokol mrežnog sloja, koji za slanje svojih poruka koristi IP pakete. Namena ICMP poruka je da pruže informacije o problemima koji se odnose na obradu IP paketa duž putanje prenosa. ICMP koristi kontrolne poruke i poruke o grešci koje se ozna?avaju brojevima od 0 do 255 (za sada ih ima oko 40). Mrežni alati, kao što su ping i traceroute, koriste ICMP protokol za svoje funkcionisanje.

Data-Link sloj

Da bi bili transportovani od izvorišnog do odredišnog hosta, paketi mrežnog sloja moraju pre?i preko razli?itih fizi?kih mreža. Fizi?ke mreže se sastoje od razli?itih tipova medijuma za prenos, kao što su bakarni provodnici, elektromagnetni talasi, opti?ka vlakna itd. Paketi mrežnog sloja nemaju implementirane mehanizme za direktan pristup razli?itim medijumima za prenos i ta funkcionalnost je implementirana na Data-Link sloju. Uloga Data-Link sloja je da pripremi pakete mrežnog sloja za transmisiju i izvrši kontrolu pristupa fizi?kom medijumu. Najzna?ajniji protokoli ovoga sloja su Ethernet, PPP, HDLC, Frame Relay, ATM itd.

Pravila filtriranja se retko definišu na Data-Link sloju, ali je mogu?e koristiti Ethernet *MAC addess access* liste, da bi se zabranio saobra?aj adresi koja je dodeljena mrežnom interfejsu, tzv. MAC adresa (media access control address).

Literatura

[1] Karen Scarfone, Paul Hoffman, Guidelines on Firewalls and Firewall Policy, Recommendations of the NIST, September 2009.

[2] Eizabet D. Zwicky, Simon Cooper & D. Brent Chapman, *Buidling Internet Firewalls*, O'Reilly Media, Second Edition, June 2000.

[3] Brian Morgan, Neil Lovering, *CCNP ISCW* Official Exam Ceerification Guide, Cisco Press, July 2007.

[4] NIST SP 800-95, *Guide to Secure Web Services*, http://csrc.nist.gov/publications/PubsSPs.html.

[5] NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)* http://csrc.nist.gov/publications/PubsSPs.html.

Autori

Zoran Mihailovi?, UNIC/Univerzitet u Kragujevcu
Bojan Jakovljevi?, RCUB/AMRES
Mara Bukvi?, RCUB/AMRES

UNIC/Univerzitet u Kragujevcu
Jovana Cvijica bb
34000 Kragujevac
Srbija

RCUB/AMRES
Kumanovska bb
11 000 Beograd
Srbija

Phone : +381 34 335709, +381 11 3031
Email : zoran@kg.ac.rs, bojan.jakovljevic@rcub.bg.ac.rs, mara@rcub.bg.ac.rs

From:
http://www.bpd.amres.ac.rs/ - **AMRES wiki**

Permanent link:
http://www.bpd.amres.ac.rs/doku.php?id=amres_cbp_wiki:amres_bpd_110

Last update: **2012/04/17 15:51**