CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Cisco ASA

CCERT-PUBDOC-2009-03-258

+CERT.hr u suradnji s LSS

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

Rezultat toga rada je i ovaj 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

Cisco Adaptive Security Appliance serije 5500 (ili jednostavnije Cisco ASA) je modularna platforma koja u svom radu koristi niz sigurnosnih funkcionalnosti, kao što su vatrozid i IPS sustav, pružajući poboljšane operativne mogućnosti provođenja i administriranja sigurnosne politike pojedine tvrtke ili organizacije. Uređaj je nastao s namjerom da se ugradi zaštita na razini infrastrukture pojedine LAN mreže proširenjem zaštite s razine mreže (na razini paketa) na razinu pojedinih programa i sadržaja.

Cisco ASA može osigurati nadzor prometa koji uključuje i pregled mreže i sadržaja, čime se zaustavljaju i potencijalne prijetnje (kao što su crvi, zlonamjerni programi, itd.) te štite svi važniji aplikacijski protokoli, servisi, krajnji korisnici te lokalna mreža općenito.

U ovom je dokumentu opisan je povijesni razvoj Cisco ASA uređaja te pojedini modeli koje je moguće nabaviti na tržištu zajedno s opisom osnovnih funkcionalnosti. Nadalje, korisnici u dokumentu mogu pronaći informacije o tome na koji se način konfigurira uređaj te koje su sigurnosne ranjivosti uočene kod ovakve opreme.

2. Cisco Adaptive Security Appliance uređaji serije 5500

2.1. Povijesni razvoj

Tvrtka Cisco Systems, Inc. je 2005. godine počela razvijati Cisco Adaptive Security Appliance uređaje serije 5500, ili kraće Cisco ASA, kao nasljednike sljedećih Cisco proizvoda:

- **Cisco PIX** – uređaj namijenjen mrežama svih veličina i zahtjeva koji obavlja funkciju vatrozida i NAT –a (eng. Network Address Translation).
  Vatrozid je sigurnosni element (mrežni uređaj ili program) smješten između lokalne i javne mreže (Interneta), a koristi se za filtriranje mrežnog prometa tako da se stvori sigurnosna zona blokiranjem i zabranom prometa po pravilima koje definira usvojena sigurnosna politika.
  NAT multipleksira promet u lokalnoj mreži i prikazuje ga kao da dolazi od jednog računala sa samo jednom IP adresom (postiže se „skrivanje" više računala na lokalnoj mreži iza jedne adrese, najčešće usmjerivača, prilikom pristupa Internetu).

- **Cisco IDP 4200** –koristi se kao IDS (eng. Intrusion Detection System) sustav
  IDS sustavi se koriste za detekciju neuobičajenih i/ili nedozvoljenih aktivnosti na računalima i mrežama. Svoj rad temelje na analizi dnevničkih podataka, provjeri integriteta podataka tj. datoteka, detekciji zlonamjernih programa te o tome obavještava administratora kako bi mogao primijeniti odgovarajuće akcije.

- **Cisco VPN koncentratora serije 3000** – platforma koja se koristi za omogućavanje VPN (eng. virtual private network) usluga te korištenje autentikacijskih mehanizama i kriptiranja podataka prilikom pristupa udaljenoj VPN mreži.

Radi se o novoj generaciji uređaja koji su namijenjeni proaktivnoj zaštiti mrežnih resursa, provjeri mrežne aktivnosti te stvaranju zaštićenih VPN tunela. Glavna karakteristika Cisco ASA 5500 uređaja je integriranje različitih tehnologija u jednu jedinstvenu platformu. Kako bi se postigle zahtijevane performanse u istovremenom radu različitih sigurnosnih servisa koriste se multiprocesorske tehnologije koje uređaju omogućuju da, u isto vrijeme i bez gubitaka, obavlja funkciju vatrozida, IPS uređaja i VPN koncentratora.

Slika 1. Cisco ASA serija proizvoda

Izvor: Cisco Systems

2.2. Modeli uređaja Cisco ASA

U razdoblju od 2005. godine do danas razvijena su različita izdanja i modeli ASA uređaja, namijenjenih različitim korisnicima (ovisno o njihovim potrebama). Tako postoje modeli koji se koriste za zaštitu manjih tvrtki, udaljenih ureda te tvrtki srednje veličine i velikih poslovnih ureda.

U nastavku slijedi opis tih modela i njihovih karakteristika:

Model	5505	5510	5520	5540	5550	5580-20	5580-40
Godina	2006.	2005.	2005.	2005.	2006.	2008.	2008.
CPU	AMD Geode LX	Intel Celeron	Intel Pentium 4 Celeron	Intel Pentium 4	Intel Pentium 4	AMD Opteron (2 CPU, 4 cores)	AMD Opteron (24CPU, 8 cores)
CPU brzina	500 MHz	1,6 GHz	2,0 GHz	2,0 GHz	3,0 GHz	2,6 GHz	2,6 GHz
RAM	256 MB	256 MB	512 MB	1 GB	4GB	8 GB	12 GB
Chipset	Geode CS5536	-	Intel 875P Canterwood	-	-	-	-
Flash memorija	64 MB	64 MB	64 MB	64 MB	64 MB	1 GB	1 GB
Max broj sučelja	3/20	500/100	150	200	250	-	-
Podrška za modularna proširenja	SSC	CSC-SSM, AIP-SSM, 4GE-SSM	CSC-SSM, AIP-SSM, 4GE-SSM	CSC-SSM, AIP-SSM, 4GE-SSM	-	da	da
Podrška za SSL VPN – broj veza	Da - 25	Da - 50	Da - 750	Da - 250	Da- 500	Da – 1000	Da-1000

Tablica 1. Modeli Cisco Adaptive Security Appliance uređaja serije 5500

Svim je modelima zajedničko da imaju jednaki oblik kućišta, a razlikuju se prema funkcionalnostima koje podržavaju te mogućnosti proširenja dodatnim modulima.

Naredna tablica nudi pregled performansi sustava:

Model	5505	5510	5520	5540	5550	5580-20	5580-40
Propusnost kod prijenosa čistog teksta, Mbit/s	150	300	450	650	1,200	5,000	10,000
AES/3DES propusnost, Mbit/s	100	170	225	325	425	1,000	1,000
Max broj simultanih veza	10,000/ 25,000	50,000/ 130,000	280,000	400,00	650,00	1,000,000	2,000,000
Max broj SSL VPN sjednica	25	250	750	2,500	5,000	10,000	10,000
Max propusnost kod VPN veza	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps	1 Gbps	1 Gbps
VPN balansiranje prometa	ne	Uz licencu	da	da	da	da	da

Tablica 2. Pregled performansi Cisco Adaptive Security Appliance uređaja serije 5500

Pojašnjenje tablice: VPN balansiranje prometa (eng. load balancing) predstavlja mehanizam za distribuciju VPN sjednica na definirane VPN poslužitelje (u slučaju kada je više Cisco ASA uređaja spojeno u grozd). Na taj se način osigurava da IP adresa predviđena za VPN vezu bude uvijek dostupna te da se osigura redundantnost sustava.

3. Strategija samoobrambene mreže

Nova generacija interaktivne poslovne komunikacije i kolaboracijskih tehnologija povećava učinkovitost i fleksibilnost svih tipova organizacija. Međutim, usporedo s tim pojavljuje se niz sigurnosnih rizika. Iz tog razloga, tijekom godina, tvrtka Cisco Systems Inc. razvija niz usluga za sprječavanje mrežnih sigurnosnih prijetnji u sklopu razvoja tzv. samoobrambene mreže (eng. Self-Defending Network)

Slika 2. Samoobrambena mreža

Izvor: Na temelju izvornika sa službenih stranica tvrtke Cisco

Strategija za razvoj spomenute mreže uključuje podršku za:

1. Zaštitu mreže – uključuje programe i servise koji obavljaju funkcije vatrozida (eng. firewall), pružaju podršku za virtualne privatne mreže (VPN) i sustave za sprječavanje neovlaštenih aktivnosti (IPS).
2. Zaštitu sadržaja – uključeni su servisi za zaštitu web pristupa sandučiću elektroničke pošte programa koji se koriste preko Interneta, sustava kojima se razmjenjuju poruke u stvarnom vremenu (eng. instant messaging system), i dr.
3. Zaštitu programa – uključena podrška za XML i HTML provjeru podataka
4. Napredno upravljanje sustavom – centralizirani nadzor nad cijelim sustavom, provjera identiteta korisnika te integriranje sigurnosne politike pojedine tvrtke.

Opsežna strategija koja uključuje samoobrambene mreže ne samo da omogućuje organizacijama zaštitu od pojedinih sigurnosnih prijetnji nego, također, nudi sustav koji se kontinuirano može mijenjati i prilagođavati aktualnoj situaciji. Spomenute usluge pridonose uspješnijem prepoznavanju, sprječavanju i prilagođavanju sigurnosnim prijetnjama kao i primjenu u različitim mogućim scenarijima.

Samoobrambena mreža, za poslovnu zaštitu pruža napredno praćenje i provjeru svih parametara uz istodobno minimiziranje rizika IT zaštite, smanjenje administrativnih IT troškova te smanjenje ukupnih troškova posjedovanja.

Cisco Adaptive Security Appliance uređaji serije 5500 jest modularna platforma predviđena za male, srednje i velike tvrtke. Elementi i funkcionalnosti ugrađene u ove uređaje su razvijane kako bi bile dio opisane Cisco samoobrambene mreže.

Pregled tih funkcionalnosti slijedi u nastavku.

3.1. Vatrozid (eng. firewall)

Od pojave usmjerivača (80-ih godina prošlog stoljeća) vatrozid je postao uobičajeni sigurnosni dio svake mreže. Kao što je već spomenuto, vatrozid predstavlja skup mehanizama koji propuštaju samo željeni promet između lokalne mreže i Interneta ili neke druge lokalne mreže. Velika većina njih svoj rad temelji na filtriranju mrežnog prometa na drugom i trećem sloju OSI modela (podatkovni i mrežni sloj). Budući da je upotreba računala te dostupnost Interneta (preko kojeg se koristi niz programa kao što su npr. webmail ili peer-to-peer programi za preuzimanje raznih sadržaja preko mreže) s vremenom postajala sve veća, proporcionalno je rastao i broj mogućih sigurnosnih prijetnji.

Spomenuti programi i servisi, koji su dostupni putem Interneta, koriste uobičajene priključne točke (eng. port) preko kojih se zatim odvija razmjena podataka, što vrlo često iskorištavaju zlonamjerni korisnici kako bi pristupili lokalnoj mreži i/ili računalu te izveli napad. Iz tog je razloga proizašla potreba za provjerom prometa i na podatkovnom sloju (sedmi sloj OSI modela). Upravo opisanu funkciju primjenjuje vatrozid koji je ugrađen u Cisco ASA uređaje, gdje se promet filtrira prema korištenim protokolima (HTTP, FTP, PPTP i dr.) pa čak i prema samim vrstama datoteka koje se prenose mrežom.

Bitno je istaknuti kako je pritom moguće vatrozid postaviti da obavlja funkcije u skladu sa sigurnosnom politikom tvrtke: postavljanjem pravila za pojedinačne korisnike i grupe, te obzirom na vrstu sadržaja koja se pregledava i koristi.

3.1.1. CSC - SCM modul

Jedan od novijih modula koji je moguće ugraditi u Cisco ASA uređaje je CSC-SSM (eng. Content Security and Control security services module), koji svojim radom nadopunjuje funkcije vatrozida.

Ovaj modul osigurava niz tzv. Anti-X usluga koje uključuju zaštitu od zloćudnih programa, filtriranje neželjene pošte i web sadržaja (anti-spam i anti-phishing), blokiranje datoteka i zaštitu od špijunskih programa (anti-spyware).

Dakle, može se reći kako automatski omogućuje provjeru i čišćenje e-mail poruka te internetskog web prometa te preuzimanje zaraženih datoteka i/ili programa. Osim toga, dostupna je i dodatna funkcionalnost filtriranja sadržaja prema URL nizovima (web adresama) kako bi se spriječio pristup nedozvoljenim web stranicama.

Ovaj je modul prvotno bio namijenjen korištenju u javnim ustanovama kao što su škole i knjižnice kako bi se osiguralo sljedeće:

1. Onemogućavanje pristupa sadržajima koji se smatraju neprikladnima za maloljetne osobe (neprimjerene slike, dječja pornografija, itd.).
2. Za nadgledanje *online* aktivnosti malodobnih osoba.
3. Za primjenu sigurnosne politike kod razmjene elektroničke pošte, RT (stvarno-vremenske) elektroničke komunikacije (npr. trenutne poruke i tzv. „chat“ sobe) i definiranja postavki za sprječavanje neovlaštenog pristupa.

3.2. Sustavi za sprječavanje neovlaštenih aktivnosti

IPS sustavi (eng. Intrusion Prevention System) štite računalne mreže podižući sigurnosnu zaštitu na višu razinu: kada se paket pojavi, IPS ga analizira i odlučuje da li predstavlja prijetnju.

U svom radu IPS sustav koristi tzv. listu pravila (koja uključuje heurističku analizu podataka, analizu pojedinih protokola, analizu neuobičajenih vrijednosti u zaglavljima paketa, i dr.) - paketi koji stignu na IPS sučelje se uspoređuju sa spomenutom listom te ovisno o tome, paket se prosljeđuje dalje u mrežu ili odbacuje. Cisco IPS koristi tri tipa pravila:

1. ugrađena pravila od strane proizvođača koja se ne mogu mijenjati,
2. ugrađena pravila kojima se mogu mijenjati parametri i
3. korisnički potpisi koje definiraju administratori.

Pravovremenom analizom paketa koji su namijenjeni pojedinim programima (tj. prije nego dođu do istoga) IPS osigurava pravovremeno uočavanje te sprečavanje nedozvoljenih aktivnosti.

Ovi sustavi transparentno ispituju mrežni promet duž svih sedam razina OSI mrežnog modela, pružajući zaštitu, između ostalog i od:

- napada temeljenih na mrežnom protokolu,
- crva,
- P2P napada,
- DoS/DDoS napada,
- SQL ubacivanja,
- Phishing-a,
- prepisivanja spremnika i
- XSS napada.

Sigurnosni napadi pojedinaca mogu izuzetno ugroziti poslovanje organizacija bilo da utječu na pohranjene informacije ili na samu mrežnu opremu. Prednosti Cisco ASA IPS sustava sastoje se u sljedećem:

- Integriranost: u sklopu jednog uređaja integriran je sustav vatrozida, IPS te VPN sustav.
- Kolaboracija: suradnja s vatrozidom prilikom ispitivanja prometa.
- Prilagodljivost: redovnim ažuriranjem IPS rješenje se brzo prilagođava novim situacijama i reagira na potencijalne opasnosti.

3.2.1. AIP SSM modul

U pojedine modele Cisco ASA uređaja moguće je ugraditi dodatni modul - AIP SSM, koji uključuje podršku za IPS sustave, sa svim mogućnostima kako bi se zaustavio pristup zlonamjernim paketima (uključujući crve, zloćudne programe i trojanske konje) prije nego što naškode uređajima i računalima u lokalnoj mreži. Automatski provodi naprednu analizu podataka na mreži (2-7 sloj OSI modela, prema IP adresama, broju priključka, vrsti prometa, itd.) i odbacuje „opasne" podatke te štiti mrežu od kršenja postavljenih sigurnosnih pravila. Osim toga, ugradnjom spomenutog modula postiže se i ubrzanje rada IPS-a, što u konačnici poboljšava i same performanse sustava općenito.

3.2.2. Razlike vatrozida i IPS-a

- Vatrozid može primijeniti pristupne ACL (eng. Access Control list) liste , pri čemu svaka lista ima svoj skup pravila na temelju kojih se odvija filtriranje prometa. Te liste su aktivne od onog trenutka kad se uspostavi pojedina sjednica. Za razliku od toga, IPS sustav provjerava svaki paket koji dođe na njegovo sučelje i na svakom primjenjuje sve predefinirane sigurnosne postavke.
- Vatrozid omogućuje funkcionalnosti NAT-a, preusmjeravanja priključaka (eng. port forwarding) i preusmjeravanja prometa, što IPS ne može.
- Vatrozid predstavlja zaštitu koja odvaja jednu mrežu od druge (npr. LAN od WAN mreže), dok se IPS postavlja na ulasku u LAN mrežu filtrirajući tako promet koji dobije od vatrozida

3.3. SSL/IPSec VPN funkcionalnost

Većina današnjih tvrtki ima zaposlenike (udaljeni djelatnici, poslovni partneri, itd.) koji imaju potrebe pristupati pojedinim podacima, informacijama ili drugim mrežnim resursima. Cisco ASA nudi dvije osnovne metode za uspostavu virtualne privatne mreže, i to bez potrebe za ugradnjom specijaliziranog sklopovlja:

1) SSL rješenje

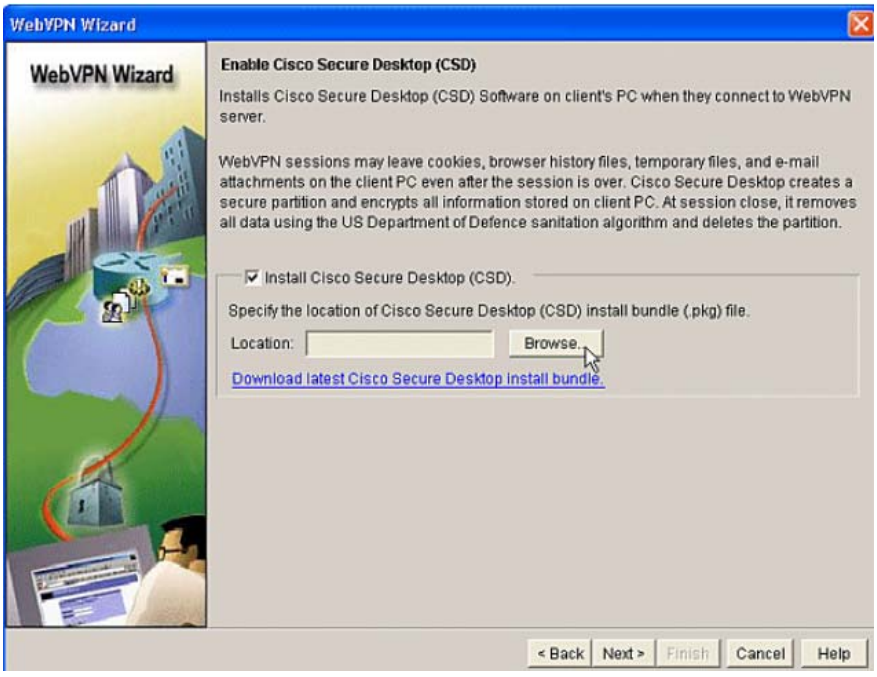
Omogućuje dvije vrste pristupa:

a) **Pristup korištenjem web preglednika**

U ovom slučaju korisnik ne mora imati instaliran nikakav dodatni program na računalu preko kojeg pristupa željenoj mreži , a spajati se može sa svih mjesta koji imaju pristup Internetu (web kiosci, privatna prijenosna računala, računala u knjižnicama i drugim javnim ustanovama). Na taj se način pojednostavljuje način primjene i smanjuju potrebna ulaganja u informacijski sustav i osoblje. Pritom se korisnik može spajati korištenjem preglednika kao što su Internet Explorer, Firefox, Opera, Safari i Packet Internet Explorera, a moguće je pristupiti programima tvrtke koja imaju web sučelje, e-mail sustavu i datotečnim sustavima. Ovaj način spajanja ponajviše koriste poslovni partneri kako bi pristupili određenim podacima neke tvrtke.

b) **Pristup pomoću instaliranog Cisco VPN klijenta**

Omogućen je pristup svim podacima tvrtke (programima i poslužiteljima). Ovaj tip rješenja uglavnom koriste djelatnici neke tvrtke koji rade na udaljenim mjestima, a imaju potrebe za pristupom svim resursima koji bi im bili na raspolaganju da se nalaze u lokalnoj mreži tvrtke. Dodatna funkcionalnost koja je na raspolaganju jest Cisco Secure Desktop (CSD) koji pruža dodatnu zaštitu kod VPN sjednice. Ova funkcionalnost omogućuje zaštitu tijekom razdoblja razmjene podataka stvaranjem sigurnog virtualnog korisničkog sučelja i čišćenja podataka (poslije povezivanja). Na taj način se brišu svi tragovi potencijalno osjetljivih informacija (kao što su kolačići, e-mail prilozi, pristupna lozinka, podaci iz priručne memorije, i dr). Kako bi se CSD mogao koristiti potrebno je imati licencu za Cisco CSD Manager kojim se upravlja preko ASDM-a, o kojem će biti više riječi u sljedećem poglavlju.



Slika 3. Cisco Secure Desktop

2) IPSec rješenje

Kao što i sam naziv kaže, ovo rješenje se temelji na primjeni IPSec protokola. Njegova je arhitektura opisana dokumentom RFC 2401, a u poslovnom svijetu SSL je najčešće korišten mehanizam za siguran prijenos podataka preko javne mreže.

Za njegovo je korištenje potrebno najprije instalirati Cisco VPN klijentski program,a kod spajanja korisnik ima pristup svim podacima tvrtke.

Obje metode imaju svojih prednosti i nedostataka, a upotreba ponajviše ovisi o potrebama korisnika koji se spajaju na mrežu određene tvrtke (odnosno, kojim podacima trebaju/smiju imati pristup) te koliko ti isti podaci moraju biti zaštićeni pri prijenosu javnom mrežom (kriptiranje). Za više detalja o razlikama IPSec i SSL primjena preporuča se pogledati dokument „Usporedba VPN poslužitelja" na stranici:

http://www.cert.hr/documents.php?lang=hr

3.3.1. Program Cisco Any Connect VPN

Cisco VPN klijentski program „Cisco Any Connect VPN" za SSL i IPSec rješenja moguće je preuzeti besplatno preko Interneta. Instalacija je jednostavna i intuitivna te zahtijeva minimalan ili nikakav angažman od strane administratora mreže. Osnovne karakteristike i funkcionalnosti programa opisane su u sljedećoj tablici:

Funkcionalnost	Opis
Optimizirani pristup mreži	- Komprimiranje podataka - Podrška za SSL i IPSec protokol
Podrška za različite platforme	- Windows 2000 - XP (32-bitni i 64-bitni) - Windows Vista (32-bitni i 64-bitni) - Mac OS X Power PC i Intel 10.4 i 10.5 - Linux Intel (2.6.x jezgra)
Jednostavna administracija	- Automatsko ažuriranje programa, što smanjuje interakciju korisnika sa samim programskim rješenjem te pojednostavljuje njegovo korištenje
Napredne mogućnosti povezivanja	- Podrška za IPv4 i IPv6 - Centralizirano upravljanje sjednicama radi optimiziranja mrežnog prometa

Tablica 3. Karakteristike programa Cisco Any Connect VPN

4. Cisco Security Device Manager (ASDM)

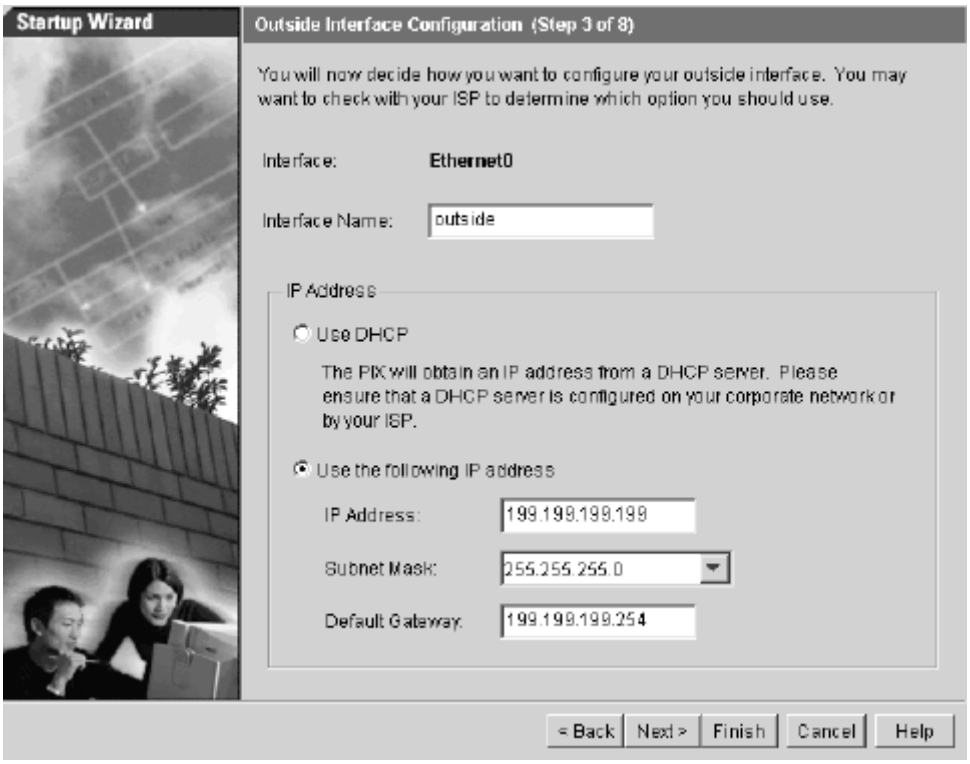
Upravljanje i nadzor nad Cisco ASA uređajima je omogućeno korištenjem programa Adaptive Security Device Manager (ASDM). Instalacija je jednostavna i intuitivna, a pokretanjem pojedinih instanci programa administratori mogu pristupati željenim komponentama uređaja te ih konfigurirati.

Trenutna je inačica programa ASDM 6.1x, dostupna za operacijske sustave:

- Microsoft Windows: Windows Vista, Windows 2003 Server, Windows XP te Windows 2000,
- Apple: Mac OS X i
- Linux: Red Hat Linux, Red Hat Enterprise Linux WS

Prilikom prvog pokretanja programa pojavljuje se čarobnjak (eng. wizard) koji administratoru olakšava postavljanje osnovnih parametara kako za privatnu mrežu tako i za pristup Internetu (slika 4). Neki od njih su:

- Privatne IP adrese – IP adresa sučelja vatrozida za privatnu mrežu.
- Javne IP adrese – IP adresa sučelja prema pružatelju podatkovnih usluga (eng. ISP – Interent Service Provider).
- NAT servisi – za pretvorbu privatne IP adrese iz lokalne mreže u javnu adresu prilikom pristupa Internetu.
- Pristupne lozinke – koriste se za povlašteni pristup funkcionalnostima vatrozida.
- DHCP – za automatsko dodjeljivanja IP adresa računalima u privatnoj mreži.
- Javni servisi –npr. mail poslužitelj, web poslužitelj, DNS poslužitelj.
- Automatsko ažuriranje.



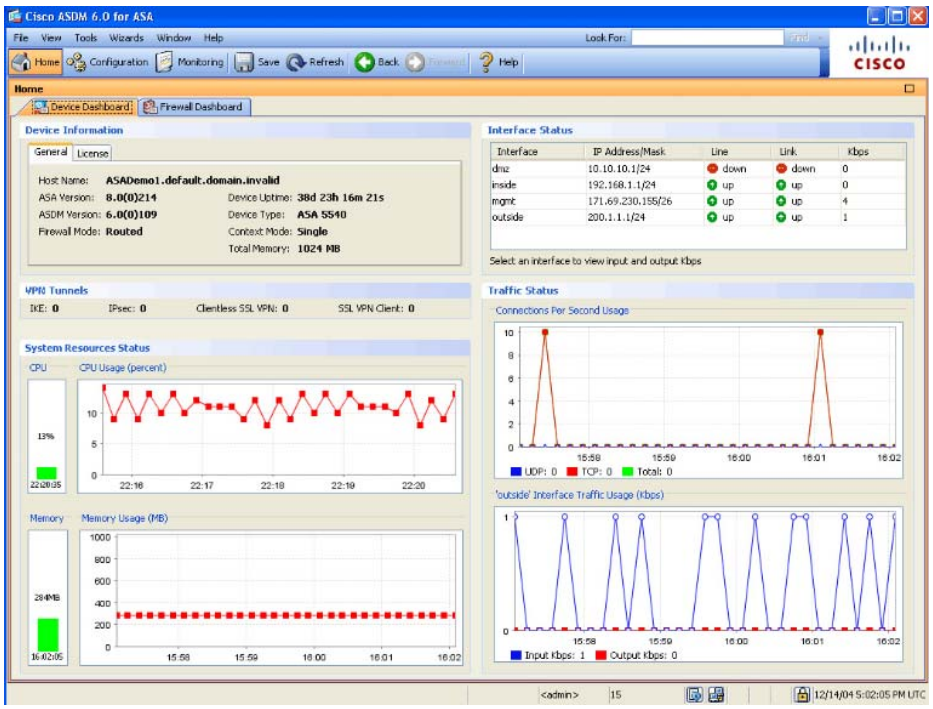
Slika 4. Konfiguriranje osnovnih parametara putem ASDM-a

4.1. Pregled mogućnosti programa

Pomoću ovog programa nudi se niz naprednih mogućnosti za konfiguriranje i nadzor sigurnosnog sustava:

- **Nadzorni ekran**

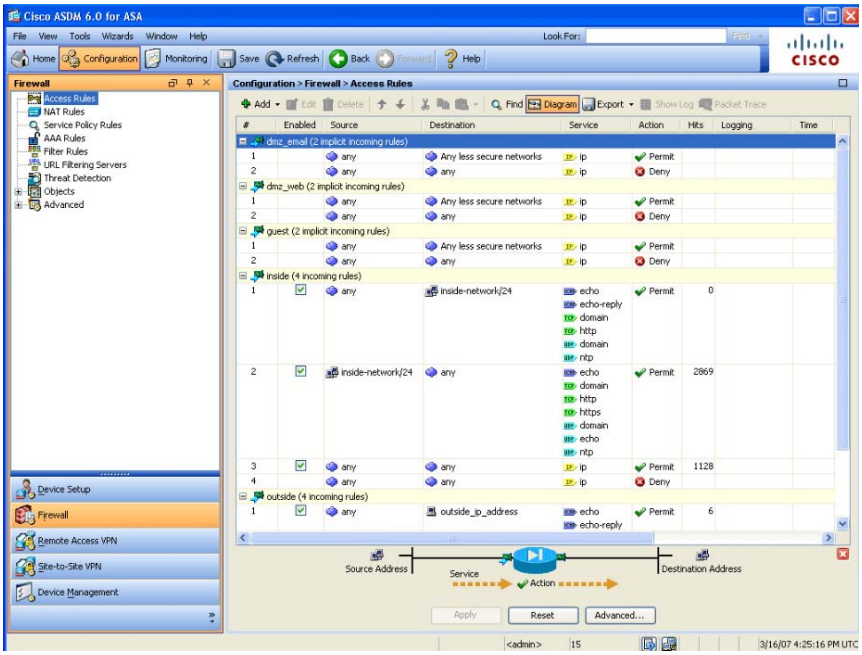
Kada je uređaj konfiguriran, Cisco ASDM prikazuje nadzorni ekran koji daje pregled cjelokupnog sustava i pojedinačne statistike uređaja i servisa (slika 5). Tako je npr. administratorima, preko grafičkog sučelja, omogućen uvid u sve ugrađene module i podatke kao što su tip uređaja, informacije o licencama, vremenu rada, itd. Za administratore sustava, u kompleksnim mrežnim okruženjima, ovakvi su podaci značajni jer u svakom trenutku mogu vidjeti RT (eng. real-time) indikatore o zauzeću resursa sustava, stanju pojedinih sučelja, zapise o VPN vezama kao i dnevničke zapise za pojedine korisnike ili adrese.



Slika 5. Prikaz statističkih podataka

- **Pregled postavki vatrozida**

Upravljanje korisnicima je pojednostavljeno na način da se stvaraju proizvoljni objekti koji se zatim svrstavaju u određene grupe na kojima se primjenjuje sigurnosna politika (npr. tko smije koristiti Internet, pojedine servise, priključke, u kojem vremenskom periodu, i dr.)



Slika 6. Sigurnosna pravila za vatrozid

- **Provjera sadržaja**

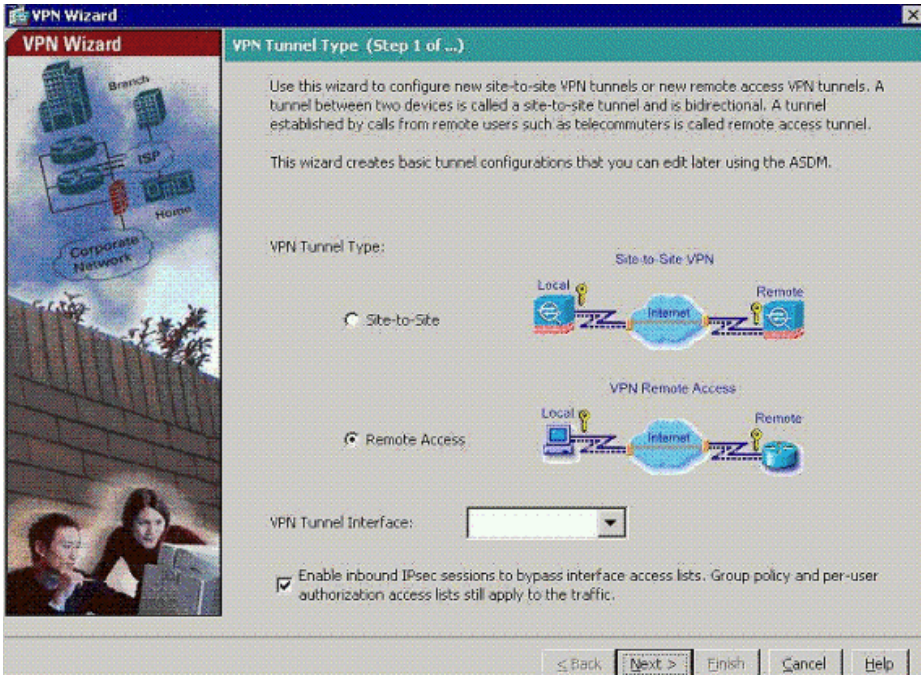
Funkcionalnost „Modular Policy Framework“ se koristi za identifikaciju mrežnog prometa kojom se zatim, prema potrebi, osigura odgovarajuća kvaliteta usluge (eng. QoS - Quality of Service). QoS predstavlja mogućnost dodjeljivanja različitih prioriteta pojedinim programima, korisnicima i tokovima podataka ili osiguranja određene razine usluge za neki tok podataka (kao primjerice minimalnog i maksimalnog propusnog pojasa).

- **Zaštićena komunikacija**

Koristi se niz metoda za autentificiranje administratora i korisnika preko RADIUS/TACACS poslužitelja. Komunikacija između ASDM i ASA se kriptira korištenjem SSL protokola i DES ili 3DES algoritma. Za dodatnu zaštitu moguće je korištenje 16 različitih tipova administratorskog pristupa kao npr. nadzor, pregled konfiguracije, dodavanje korisnika, i dr.

- **VPN pristup**

Pomoću VPN čarobnjaka omogućena je uspostava VPN veza korištenjem IPSec ili SSL protokola. Tijekom same VPN sjednice preko ASDM-a moguće je u svakom trenutku vidjeti brojne statistike i grafove koji pokazuju podatke o trajanju sjednice, količini podataka koji se prenose po sjednici i dr.



Slika 7. Konfiguriranje VPN veze korištenjem čarobnjaka

- **Zaštita pojedinih programa**

Uključuje korištenje niza alata za nadzor i zaštitu programa kojima se pristupa preko HTTP (eng. Hyper Text Transfer Protocol), FTP (eng. File Transfer Protocol), GTP (eng. GPRS Tunneling Protocol), SIP (eng. Session Initiation Protocol), H323 te SunRPC (eng. Sun Remote Procedure Call) protokola.

- **IPS funkcionalnost**

IPS se konfigurira kako bi se mreža zaštitila od različitih sigurnosnih prijetnji kao što su crvi, zloćudni programi, trojanski konji, špijunske datoteke i ostali neovlašteni ulazi u sustav.

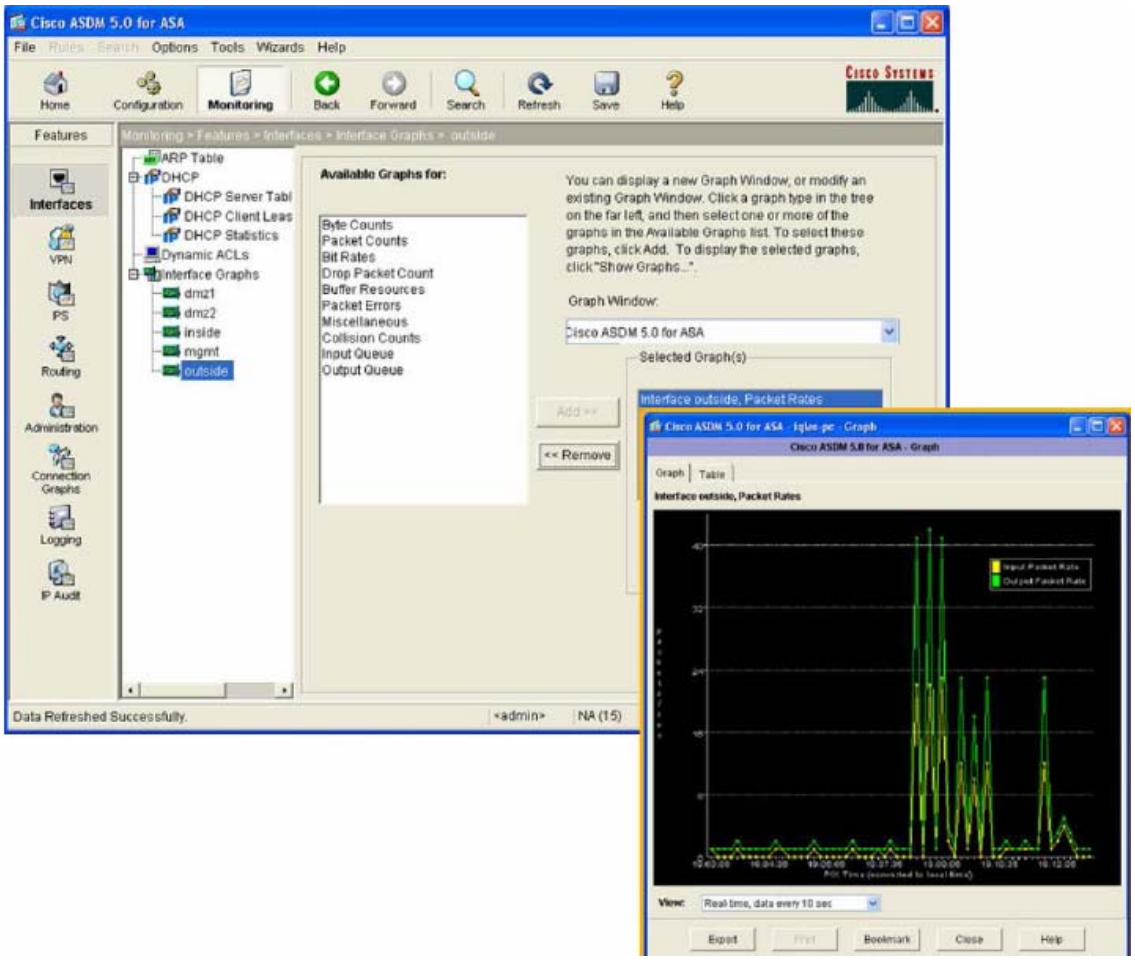
- **Packet Tracer**

Pruža postepenu analizu obrade paketa kod uređaja Cisco ASA serije 5500 i može pomoći brzoj identifikaciji i ispravljanju konfiguracijskih grešaka.

- **Analiza rada sustava**

Daje detaljnu analizu (numerički i grafički) rada sustava. Tako je moguće pregledavati:

1. Sistemski graf – CPU iskoristivost, koliko se radne memorije koristi
2. Graf za prikaz aktivnosti korisnika – AAA (eng. authorization, authentication and accounting) transakcije, URL filtriranje, NAT translacije
3. Graf za pregled rada IPS sustava



Slika 8. Analiza rada ASA uređaja

5. Pregled sigurnosnih ranjivosti

U nastavku teksta slijedi opis ranjivosti programa Cisco ASDM, inačica 5.x i 6.x. Također, slijedi i pregled ranjivosti za uređaje Cisco ASA inačice 7.x te 8.x.

Detaljniju analizu s pripadnim statistikama može se pogledati na Secunia-inim službenim stranicama:

http://secunia.com

5.1. Sigurnosni propusti aplikativne podrške

5.1.1. Cisco Adaptive Security Manager (ASDM) 5.x i 6.x

Zadnji sigurnosni propust pronađen u ovom programskom paketu zabilježen je 2007. godine. Radi se o ranjivosti niskog stupnja rizika koju je mogao iskoristiti lokalni zlonamjerni korisnik za izvođenje tzv. *spoofing* napada i pristup osjetljivim i/ili zaštićenim podacima. Proizvođač je objavio potrebne programske ispravke kako bi se problem otklonio.

Za inačicu programa Cisco ASDM 6.x, trenutno nije zabilježen niti jedan sigurnosni nedostatak.

5.2. 5.2. Sigurnosni propusti uređaja

5.2.1. Cisco Adaptive Security Appliance (ASA) 7.x

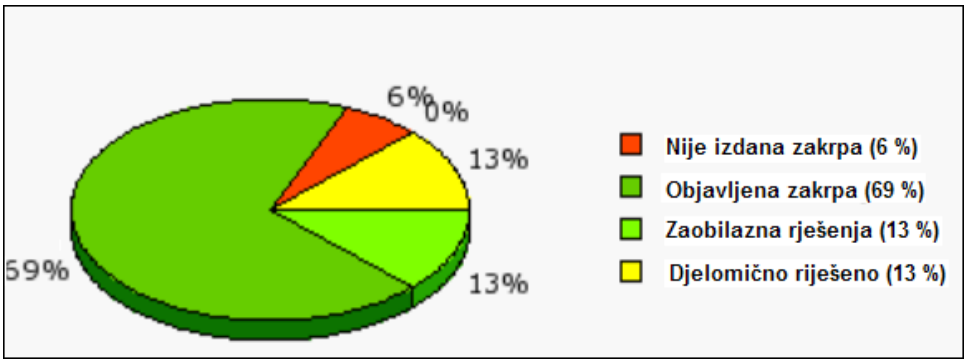
U razdoblju od 2003. do 2009. godine za ovu inačicu uređaja uočeno je 16 sigurnosnih propusta.

Sve propuste visokog i srednjeg stupnja proizvođač je u potpunosti ispravio, dok je samo jedan propust niskog stupnja riješen djelomično.

Prema stupnju rizika uočeno je sljedeće:

- Visoki stupanj rizika – niti jedan slučaj
- Srednji stupanj rizika – 63 % propusta
- Niski stupanj – 19 %
- Jako niski stupanj – 19 %

Dio propusta je ispravljen, dio je riješen djelomično, dok su neke od ranjivosti, ocijenjene jako niskim stupnjem rizika, ostale neriješene(slika 9).

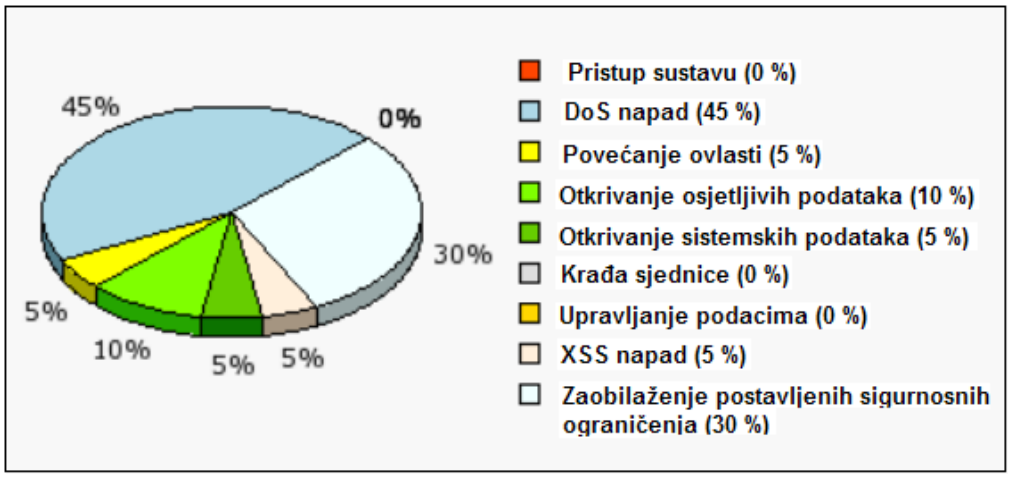


Slika 9. Podjela propusta prema objavljenim sigurnosnim zakrpama

Izvor: Secunia Security Team

U većini je slučajeva udaljeni napadač mogao zlorabiti navedene propuste (81 %), dok su lokalni napadači mogli puno manje utjecati na sigurnost sustava (19 %).

Prema vrsti napada najzastupljeniji su bili propusti koji su rezultirali zaobilaženjem postavljenih sigurnosnih ograničenja te DoS (eng. Denial of Service) stanjem (slika 10):

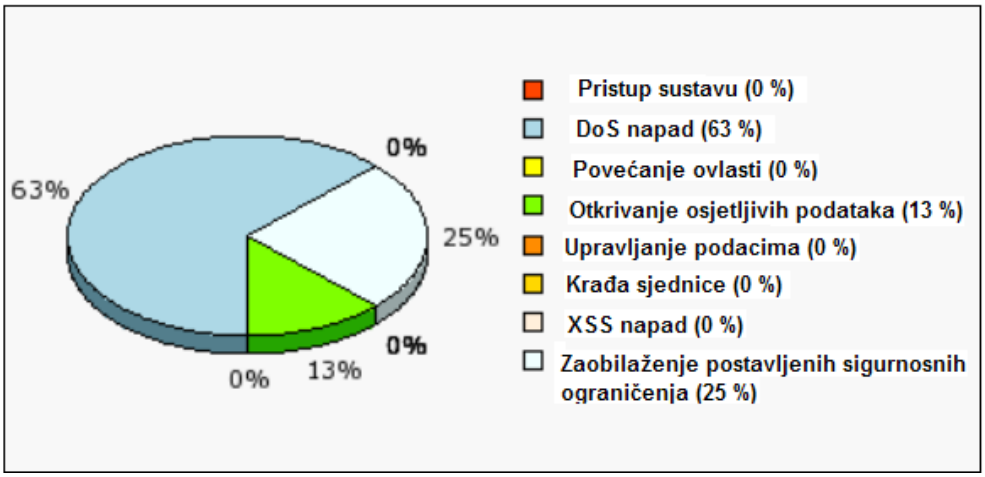


Slika 10. Podjela propusta za Cisco ASA 7.x prema vrsti napada

Izvor: Secunia Security Team

5.2.2. Cisco Adaptive Security Appliance (ASA) 8.x

Udjeli pojedinog tipa propusta prikazani su na slici:



Slika 11. Podjela propusta za Cisco ASA 8.x prema vrsti napada

Izvor: Secunia Security Team

U zadnjih šest godina (razdoblje od 2003. do 2009. godine), koliko Secunia-ini stručnjaci prate otkrivanje propusta, za Cisco ASA 8.x otkriveno je ukupno 6 sigurnosnih ranjivosti. Svi su propusti srednjeg stupnja rizika, a bitno je napomenuti kako ne postoji niti jedan prijavljeni propust za kojeg nije objavljena odgovarajuća zakrpa.

6. Zaključak

Cisco ASA serija 5500 (Adaptive Security Appliance) je nova generacija uređaja namijenjenih proaktivnoj zaštiti mrežnih resursa, provjeri mrežne aktivnosti i prometa kroz mrežu, kao i stvaranju zaštićenih VPN tunela.

Proširujući dosege Cisco-ve ASA obitelji i koristeći nove servise, koje se razvijaju u sklopu navedenog uređaja, uređaj pruža dodatne elemente zaštite za svaki tip tvrtke (od onih sa nekoliko računala i jednim ili dva poslužitelja do sustava sa više stotina korisničkih računala i nekoliko desetaka poslužitelja). Najnovije izdanje programa za Cisco ASA 8.x nudi više od 50 novih sigurnosnih funkcija koje ojačavaju ASA vatrozid na programskoj razini (Layer 7), IPS sustav, VPN pristup na daljinu, dostupnost, mrežnu integraciju i mogućnosti upravljanja. Ovaj uređaj ujedinjuje niz sigurnosnih programskih rješenja, kojima se pridonosi ukupnom smanjenju operativnih troškova i pruža manje iskusnim korisnicima mogućnost izvođenja složenih zadataka vezanih uz sigurnosne politike na globalnoj razini. Osim toga, pojednostavljuje podršku Cisco-ve sigurnosne strategije za samoobrambene mreže, što pomaže tvrtkama da prepoznaju, spriječe te se prilagode postojećim kao i novim sigurnosnim prijetnjama. Kao takav, uređaj predstavlja izuzetno jak odsječak na mreži koji učinkovito štiti lokalnu mrežu i podatke na njoj.

7. Reference

[1] Cisco , http://www.cisco.com/web/HR/solutions/ent/security_what.html , prosinac 2007.

[2] Cisco, http://www.cisco.com/web/HR/news/2006/2006_news_s09.html , prosinac 2007.

[3] Cisco , http://i.i.com.com/cnwk.1d/i/tr/downloads/home/1587052148_chapter_5.pdf, travanj 2005.

[4] Secunia , http://secunia.com/advisories/product/16163/?task=statistics , veljača 2009.

[5] Secunia , http://secunia.com/advisories/product/19143/ , veljača 2009.

[6] Secunia , http://secunia.com/advisories/product/12574/?task=statistics , veljača 2009.

[7] Cisco , http://www.cisco.com/en/US/docs/security/asdm/6_1/user/guide/csc.html , siječanj 2009.

[8] Wikipedia,http://en.wikipedia.org/wiki/Cisco_ASA_5500_Series_Adaptive_Security_Appliances, veljača 2009.