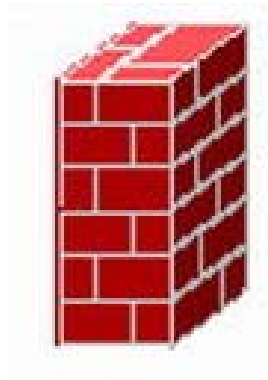


Zaštita računarskih mreža

FIREWALL



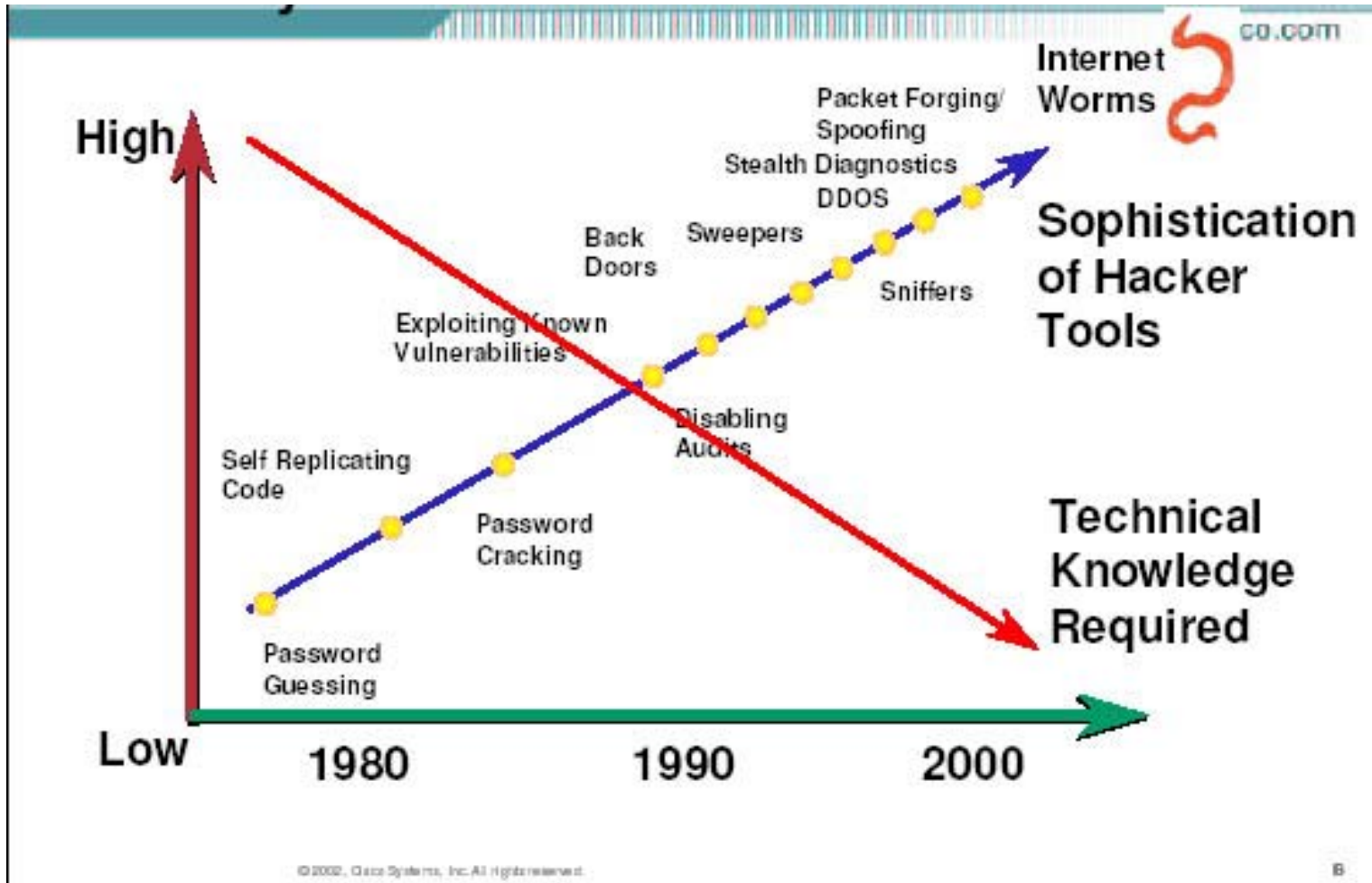
UVOD

- Sa spektakularnim rastom Interneta, kompanije koje koriste Internet za svakodnevne poslove, susrijeću se sa sve većim sigurnosnim rizicima.
 - Kako može kompanija da spriječi korisnike koji pristupaju kompanijskoj Web stranici, da pristupe drugim strogo povjerljivim resursima na privatnoj mreži?
 - Kako onemogućiti zaposlenima da pošalju strogo povjerljive informacije u spoljni svijet?
- Ovo su samo neki od primjera kako kompanijska sigurnost može biti ugrožena!

Najčešće opasnosti po računarske sisteme

- Kompjuterski virusi (Worm, Trojan ...)
- DDOS napadi (Distributed Denial of Service)
 - postoje razne vrste napada koje u zavisnosti od tipa mogu da uzrokuju nedostupnost mreže, zagušenje, izmjenu konfiguracije mrežnih komponenti, opterećenje resursa servera na mreži ...
 - **Smurf Attack**, Ping Of Death, Syn Flood Attack ...
- Vulnerability
 - Sigurnosni propusti u operativnim sistemima koje napadač može iskoristiti (sig. propust u MS SQL 2000 serveru izazvao krah 98% Interneta)

- Lakša dostupnost hakerskih alata
- Potrebno je skromno znanje za korištenje tih alata



Komponente zaštite računarske mreže

CISCO.COM

Secure
Connectivity



VPN
Tunneling
Encryption

Perimeter
Security



ACLs – IOS FW
Firewalls

Security
Monitoring



Intrusion Detection
Scanning

Identity



Authentication
Digital Certificates

Security
Management



Policy Mgmt
Device Mgmt
Directory Svcs



Načini zaštite računarskih mreža

U proteklih nekoliko godina ruter je bio sve što je stajalo između privatnih (javnih) mreža i Interneta. Ruteri koriste packet-filtering i ACL (access control list) da bi ograničili pristup nekom resursu. Ovo se pokazalo kao nedovoljno zbog slabosti koje su se pokazale kod packet-filtering-a, kao i zbog opterećenja koje ACL izazivaju na ruterima.

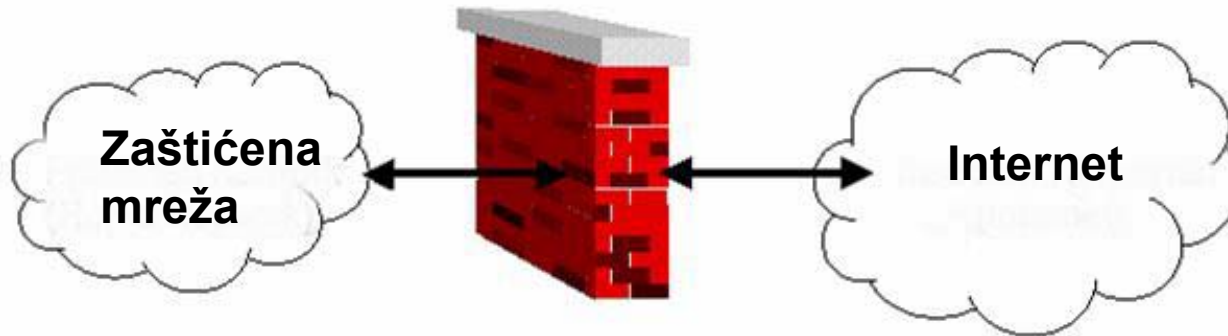
Packet-filtering – način kontrole pristupa paketima na osnovu adrese paketa (source – destination address)

Što je to Firewall

- Firewall je uređaj koji filtrira sav saobraćaj između zaštićene unutrašnje mreže i spoljne mreže kojoj se manje vjeruje.
- Uobičajeno je da se firewall nalazi na posebnom uređaju, jer je to tačka kroz koju prolazi sav saobraćaj
- Performanse su vrlo bitne, što znači da sve funkcije koje nisu vezane za firewall ne bi trebalo da se nalaze na ovom uređaju
- Firewall je izvršni kôd, a kao i svaki drugi kôd, on se može zloupotrijebiti. Iz tog razloga se kôd firewall-a izvršava na posebno namijenjenom mjestu, ili pažljivo minimizovanom operativnom sistemu.

Namjena firewall-a, način funkcionisanja

- Osnovna namjena firewall-a je da “drži” loše stvari izvan zaštićene mreže. Da bi se to postiglo, firewall implementira razne sigurnosne polise koje su tako napravljene da tačno predvide koje se loše stvari mogu desiti.



- **Primjer: polisa može biti ta da zabrani bilo koju konekciju spolja, dok su konekcije iz unutrašnje mreže prema spoljašnoj i dalje dozvoljene. Varijacija ove polise može biti da se dozvoljava pristup unutrašnjoj mreži, ali samo sa određene adrese, na tačno određenu adresu i po tačno određenim protokolima itd.**

Vrste firewall-a (Unix, NT) – prednosti i mane

- U upotrebi su najviše Unix (NT) bazirana rješenja firewall-a, koje rade na principu proxy servera. Ovi proxy serveri rade u gornjem sloju OSI nivoa 7, što im omogućava da održavaju stanje sesije (session state) kao i da podržava autentifikaciju na korisničkom nivou, za bolju sigurnost. Služe za povezivanje kompanijskih lokalnih mreža sa spoljnim mrežama koristeći specifične firewall aplikacije.
- Koristeći proxy server, korisnici dobijaju mogućnost pristupa mreži koristeći proces uspostavljanja veze, autentifikacije i autorizacije
- Proxy serveri nude veliku sigurnost iz razloga što se sesija zadržava na OSI nivou 7 (aplikativni nivo)

Vrste firewall-a (Unix, NT) – prednosti i mane

- Ali, prednost velike sigurnosti kod UNIX (NT) proxy servera zahtijeva velike performanse.
 - Funcionisanje proxy servera na 7 nivou OSI modela je vrlo intenzivan proces koji “troši” puno CPU vremena. Ovo je razlog zašto čak i jake Unix mašine (Sparc 10) koje rade kao proxy serveri, mogu da podrže samo određeni broj sesija istovremeno. Iz ovog razloga, kompanije neće moći u potpunosti da iskoriste mogućnosti brzih internet konekcija.
 - Takodje, održavanje proxy servera je prilično skupo, iz razloga veličine i ranjivosti Unix (NT) operativnih sistema (stalno održavanje i administracija sistema)

Cisco's PIX Firewall: Siguran, visokih performansi, lak za održavanje



Cisco Systems' **PIX** (**P**rivate **I**nternet **E**xchange) Firewall zadovoljava većinu sigurnosnih potreba kompanija, bez ograničenja u performansama prisutnih kod proxy servera

Cisco PIX Firewall – način rada

- Cisco's PIX Firewall nudi sigurnu i jaku zaštitu, oslobodjenu prekomjernog administriranja i rizika koji se javljaju kod Unix (NT) firewall sistema. Administrator dobija kompletne izvještaje o obavljenim logovanjima, kao i pokušaje upada na unutrašnju (zaštićenu) mrežu.
- Cisco PIX donosi veliku prednost u performansama, uvodeći način rada – *cut through proxy*. Kod ovog načina rada, Cisco isto kao i Unix, ostvaruje konekciju na 7. OSI nivou, omogućavajući autentifikaciju i autorizaciju, ali za razliku od Unix-a, odmah nakon procesa AA na nekom od za to predviđenih servera (TACACS+, RADIUS) PIX “spušta” sesiju na niži nivo, čime se ostvaruje brz i direktan saobraćaj, uz održavanje stanja sesije. *Cut Through* omogućava PIX firewall-u mnogo brži rad u odnosu na proxy servere.
- Cisco PIX takodje omogućava veliku sigurnost kroz upotrebu ASA algoritma (Adaptive Security Algorithm) i kroz upotrebu “stateful” informacija. (SA, DA, Ports, random TCP Sequence number, additional TCP flag, Hashed)
- Sve konekcije se loguju, kao i autorizovani i neautorizovani pokušaji, koristeći Syslog ili SNMP

Cisco PIX Firewall



- Cisco PIX predstavlja idealno rješenje za kompanije koje brinu o potrebi administriranja.
- Može se konfigurisati za svega nekoliko minuta, sto skraćuje *downtime*, izuzetno važnu stavku u planiranju sigurnosti mreže.
- Nije baziran na Unix-u, tako da nije potrebno svakodnevno administriranje.
- Cisco PIX se izvršava u *Flash* memoriji, i samim tim nema hard disk
- Može se konfigurisati u *Failover* modu, kada dva PIX-a rade paralelno, i u slučaju otkaza jednog, drugi u potpunosti preuzima funkcionisanje
- Podržava preko 16000 istovremenih TCP sesija

Cisco PIX firewall – podržane mogućnosti

- Specifični operativni sistem, dizajniran da obavlja glavnu funkciju – da bude firewall. Oslobodjen suvišnih stvari kojima su opterećena druga firewall rješenja (Unix, NT)
- Odlican Adaptive Security Algorithm (ASA)
- *Cut-through* proxy autentifikuje i autorizuje konekcije, ujedno poboljšava performanse
- Web interfejs za administraciju i daljinsko održavanje *PIX Security Appliances*
- Podrška do 10 ethernet interfejsa od 10BASE-T, 10/100 Fast Ethernet do Gigabit Ethernet
- *Failover* mogućnost rada sa sinhronizacijom informacija o konekcijama i radnim konfiguracijama

...

...

- NAT (Network Address Translation) po RFC 1631 specifikaciji
- Port Address Translation (PAT) – proširuje adresni prostor – jedna IP adresa podržava više od 64,000 hostova
- Podrška za IPSec i L2TP-PPTP vrste VPN-ova
- Podrška za URL filtriranje
- Mail guard zamjena za mail relay server u DMZ dijelu unutrašnje mreže
- Podrška za većinu autentifikacijskih protokola. TACACS+, RADIUS i Cisco ACS kompatibilnost i integracija

...

...

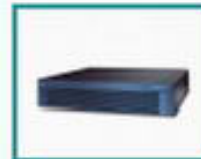
- Flood Guard & Fragmentation Guard štite od DDOS napada (Ping of Death)
- Podrška za napredne VoIP standarde, uključujući SIP, H.323 i dr.
- Java blocking zaustavlja potencijalno opasne Java aplete (koji nisu kompresovani ili arhivirani)
- Proširene AAA mogućnosti
- Mogućnost podešavanja protokola i imena portova
- Integracija sa Cisco Intrusion Detection Systems za izbjegavanje poznatih zlonamjernih IP adresa

...

...

- Poboľjšano podešavanje Syslog poruka
- Simple Network Management Protocol (SNMP) i Syslog za udaljenu administraciju
- Pouzdan Syslogging korištenjem TCP ili UDP

PIX Firewall Product Line Overview

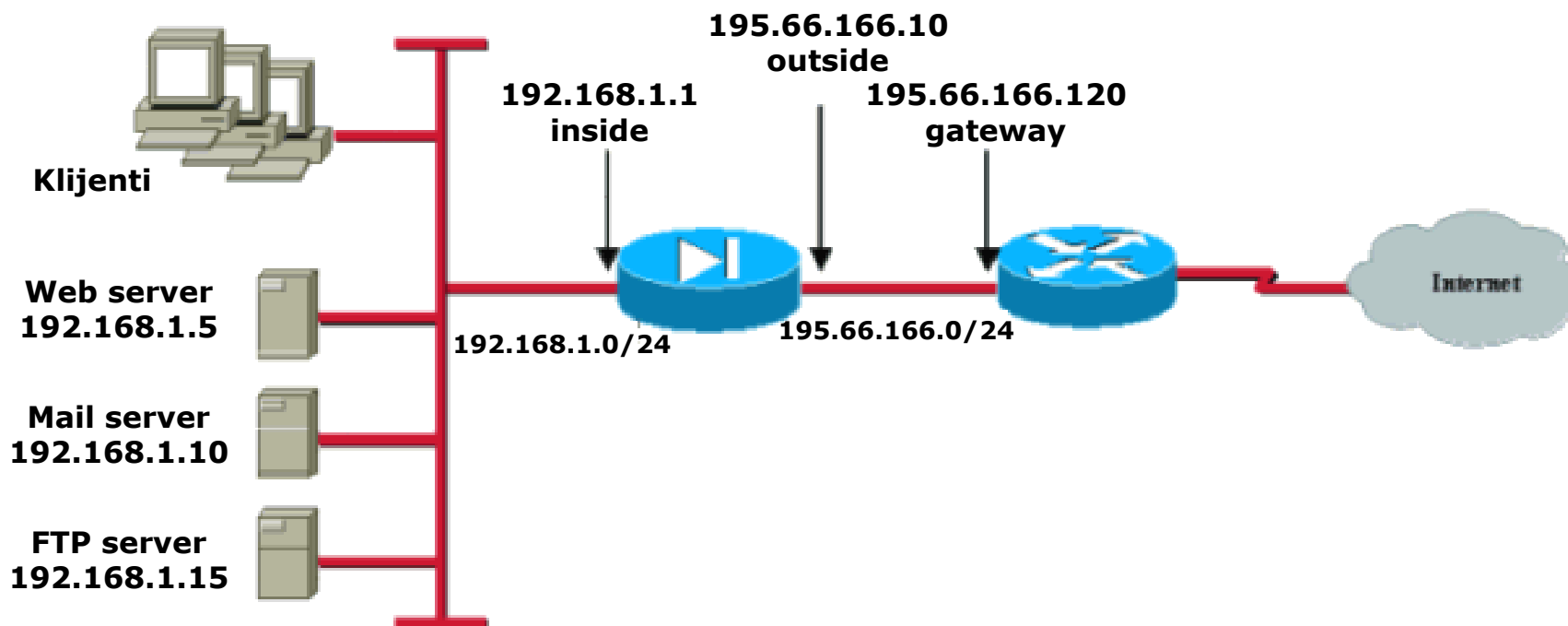


Model	501	506E	515E-UR	525-UR	535-UR
Market	SOHO	ROBO	SMB	Enterprise	Ent., SP
Licensed Users	10 or 50	Unlimited	Unlimited	Unlimited	Unlimited
Max VPN Peers	5	25	2,000	2,000	2,000
Size (RU)	< 1	1	1	2	3
Processor (MHz)	133	300	433	600	1 GHz
RAM (MB)	16	32	64	256	1 GB
Max. Interfaces	1 10BT + 4 FE	2 10Base T	6	8	10
Failover	No	No	Yes	Yes	Yes
Cleartext (Mbps)	10	20	188	360	1.7 Gbps
3DES (Mbps)	3	16	63	70	95

Cisco PIX - konfiguracije

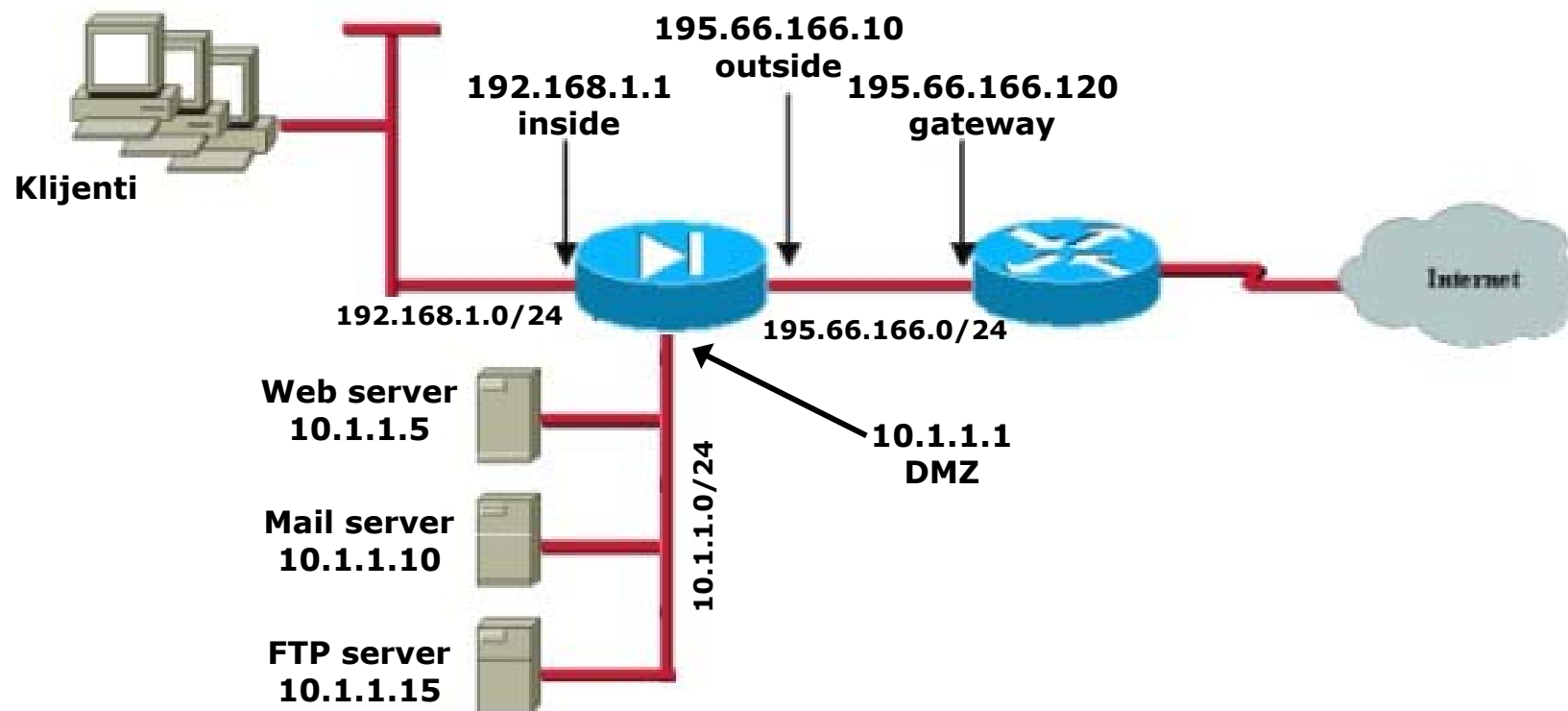
Pri dizajniranju sigurne mreže, u zavisnosti od zahtjeva korisnika, može se napraviti više konfiguracija. Dvije koje su najčešće u upotrebi su:

- Interna (zaštićena) mreža - Internet (“spoljni svijet”)



Cisco PIX - konfiguracije

- Interna (zaštićena) mreža – DMZ – Internet (“spoljni svijet”)



Appendix

- Primjer SYSLOG-era sa prikazom dijela log-a ([syslog.pdf](#))
- Primjer konfiguracije PIX firewall-a:
Interna (zaštićena) mreža - Internet (“spoljni svijet”) ([konfiguracija1.pdf](#))
- Primjer konfiguracije PIX firewall-a:
Interna (zaštićena) mreža - DMZ - Internet (“spoljni svijet”) ([konfiguracija2.pdf](#))
- NAT (Network Address Translation) po RFC 1631 specifikaciji ([rfc1631.pdf](#))