கணினியும் தீச்சுவரும்

ஆக்கம்: சுப. இரத்தினகிரி.

நம் அன்றாட வாழ்வில் கணினியின் பங்கு அதிகரித்துக் கொண்டே வருகின்றது என்பதை நாம் அனைவருமே அறிவோம். இந்தப் பேருலகம் ஒரு கிராமமாய்ச் சுருங்கியதற்கு கணினியும் ஒரு முக்கியக் காரணம் ஆகும். எண்ணிக்கையில் கணினிகள் பெருகி வந்தாலும் அவற்றின் இடையே இருக்கும் இடைவெளியைக் குறைக்க உதவுவது **இணையம்** என்றொரு பெருங்கடல் என்றால் அது மிகையாகாது.

இதெல்லாம் தான் எங்களுக்கு ஏற்கனவே தெரியுமே என்று தானே சொல்கின்றீர்கள். மர்பி தம் விதிகளில் சொல்வது போல "20 ஆண்டுகளாய் 20 மனிதர்கள் செய்ய முடியாத தவறைக் கூட இரண்டே விநாடிகளில் ஒரு கணினி செய்து விடும்". என்பதும் உண்மையே.

நல்லது எதிலெல்லாம் இருக்கின்றதோ அதிலெல்லாம் தீமையைக் கலப்பது மனிதனின் மூளையல்லவா?

இணையத்திலும் தீமைகள் விரவிக் கிடக்கின்றன. இணையம் என்பது மின்கடத்தி போல் தகவல் கடத்தி என்று வைத்துக் கொள்ளலாம். கடத்தியில் பிரச்னை இல்லை. ஆனால் அது எதைக் கடத்துகின்றது என்பதில் தான் பிரச்னையே.

திரு. பாலச்சந்தர் அவர்களின் ரயில் சிநேகம் என்றொரு தொலைக்காட்சித் தொடர் வெளிவந்தது அநேகம் பேருக்குத் தெரிந்திருக்க நியாயமில்லை! அந்தத் தொடரின் தலைப்புப் பாடலாக வைரமுத்துவின் வைர வரிகளில்,

"இந்த வீணைக்குத் தெரியாது அதைச் செய்தவன் யாரென்று,
இந்தப் பிள்ளையும் அறியாது இதைத் தந்தவன் யாரென்று,
வீணையில் படிக்கும் ராகங்கள் வீணை அறியாது..."

என்று செல்லும் வரிகளில் குறிப்பிடுவது போல், இணையம் அறியாது

தான் எதைத் தருகின்றோம் என்று!

அதில் நமக்குத் தேவையான தகவல்களும் இருக்கலாம். அல்லது வைரசுகள், நச்சுப் புழுக்கள், ஒற்று மென்பொருட்கள், குப்பை கூளங்கள் வரும் மின்னஞ்சல்கள், தகாத விளம்பரங்கள், 108 பேருக்கு அனுப்பு என்ற கட்டளைகள், 10000 கோடி ரூபாய் கொஞ்ச நாள் வைத்திருக்கின்றீர்களா என்று கேள்விகள் என்று பல்வேறு பிரச்னைகள் இணையத்தில் தொடர்பு கொள்வதால் நமக்கு இலவசமாய் கிடைக்கின்றன. அதற்காக இணையமே நான் உபயோகிக்கப் போவதில்லை என்றால், மூட்டைப்பூச்சிக்காக வீட்டைக் கொளுத்திய கதை தான்.

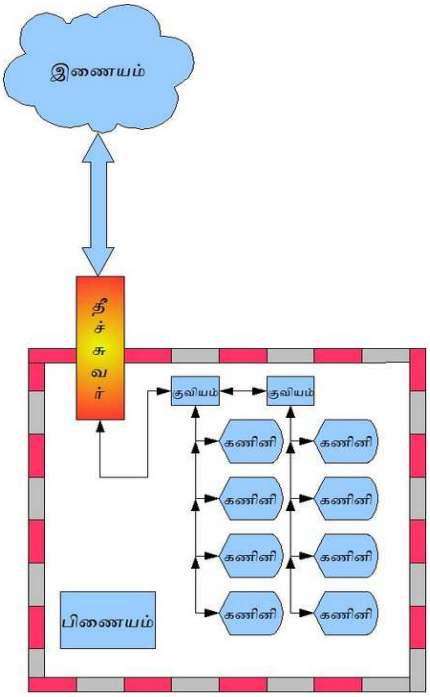
எனவே பாதுகாப்பாய் இணையத்தை உபயோகித்து நமக்குத் தேவையான தகவல்களை மட்டும் பெறுவது என்பது ஒரு கலை. அந்தக் கலைக்கு உபயோகமாய் இருக்கும் ஆயுதமே **தீச்சுவர்** (Firewall) ஆகும். இந்தக் கட்டுரையில் தீச்சுவர் பற்றிச் சிறிது பார்ப்போம்.

தீச்சுவர் என்றால் என்ன?

தீச்சுவர் என்பது இணையத்திலிருந்து (WWW) தனியாகச் செயல்படும் ஒரு பிணையத்தைப் (Private Network) பிரித்து உள்ளே வரும் தகவலையோ, வெளிச் செல்லும் தகவலையோ சரி பார்க்கும் ஒரு காவலாளி ஆகும். தீச்சுவர் ஒரு மென்பொருளாகவோ வன்பொருளாகவோ இருக்கலாம்.

நம் இல்லத்தில் நான்கு புறமும் சுவர் கட்டி வைத்திருப்பது எதற்காக? நாம் பாதுகாப்பாய் இருப்பதற்கும், அடுத்தவர் உள்ளே வந்து விடாதிருக்கவும் தானே? அதற்கு உதவுவது கதவு. இங்கே தீச்சுவரும் கதவின் பணியே செய்கின்றது. எனவே **தீச்சுவர் வைத்திருப்பதன் மூலம் நம் தகவல் பரப்பை ஓரிடத்தில் குவித்துச் சரி பார்த்துப் பின் வெளியே அனுப்புவது அல்லது உள்ளே விடுவது ஆகிய பணியைச் செய்கின்றோம்**.

இந்தப் படத்தைப் பாருங்கள். இணையத்திலிருந்து வரும் தகவலை தீச்சுவர் வழியே பிணையத்திற்கு அனுப்பி அங்கிருக்கும் கணினிகள் பகிர்ந்து கொள்கின்றன.



தீச்சுவர் வைத்திருந்தால் போதுமா? என் கணினியை இணையத்தில் எந்த ஒரு நச்சுப் பொருளும் பாதிக்காதா? என்று கேட்டீர்களானால் விடை இல்லை என்றே வரும்! ஏற்கனவே நான் சொன்னது போல தீச்சுவர் என்பது ஒரு கதவு போன்றது. எனவே திருடன் (நச்சுப் பொருள்) சரியான சாவி கொண்டு வந்தாலோ அல்லது கதவை உடைத்து உட்புகுந்தாலோ உள்ளே நுழைந்து விட வாய்ப்பிருக்கின்றது. நல்ல வேளையாக இங்கே கதவை உடைப்பது என்பது சாத்தியமில்லை. எனவே சாவி தான் மிக முக்கியமானது. எந்தச் சாவியைக் கொண்டு வந்தாலும் திறக்க முடியாத பூட்டு எப்படி தயாரிப்பது என்பதுவே இந்தக் கட்டுரையின் நோக்கமாகும்.

இணையம் வேலை செய்வது எப்படி?

இணையத்தில் நீங்கள் மின்னஞ்சல் அனுப்பினாலும் சரி, கோப்பு அனுப்பினாலும் சரி, அல்லது ஒரு வலைப்பக்கத்தில் உலவினாலும் சரி, இணையத்தைப் பொருத்த வரை அது ஒன்று தான். எதுவானாலும் இணையத்தைப் பொருத்தவரை இருமைத் (binary) தகவல்கள் ஒரு புறமிருந்து இன்னொரு புறம் செல்கின்றது அவ்வளவே!

இதில் எங்கிருந்து எங்கே செல்கின்றது என்று தபால் நிலையத்தில் போல் குறித்து வைத்து இணையம் அனுப்புகின்றது. அதைப் பொட்டலம் (Packets)

என்பார்கள். ஆம், நம் தகவல்களும் சிறு சிறு பொட்டலங்களாகக் (65535 பைட்டுக்கள் அளவில் - IPV4) கட்டப்பட்டு இணையத்தில் அனுப்பப்படுகின்றன. ஒவ்வொரு பொட்டலத்திலும் அதை அனுப்பும் இணைய முகவரி (ஐபி), சேரும் இணைய முகவரி, நெறிமுறை என பல தலைப்புத் தகவல்களுடன் (Header information) நம் தகவல்களும் இருக்கும்.

முதல் தலைமுறை தீச்சுவர்கள் வெறுமனே இந்தப் பொட்டலத்தினைப் பிரித்துப் பார்த்து நமக்குத் தேவையானது தானா என்று வடிகட்டி (Packet Filters) சரி பார்ப்பதாகவே இருந்தன. பின்னால் பல வசதிகள் சேர்க்கப்பட்டு தற்போது கள்ளனைப் போல் காப்பானும் வளர்ந்து கொண்டே வருகின்றது!

இனி தீச்சுவரை எப்படி அமைப்பது? என்னென்ன செய்து கணினியைக் காக்கலாம் என்று கண்டறிவோம்.
சில கலைச்சொற்களை அறிந்து கொள்வோம்.

1. Port - துறைமுகம். நம் நாட்டிலுள்ள துறைமுகம் போல தான். நாட்டில் பல துறைமுகங்கள் இருப்பது போல ஒரு கணினியிலும் பல துறைமுகங்கள் இருக்கின்றன. நாட்டுத் துறைமுகத்துக்குப் பெயர் இருப்பது போல், இந்தத் துறைமுகத்துக்கும் எண்களால் பெயருண்டு. உதாரணமாக 80, 110, 25, 3306, 8080,21 போன்றவை நம் தூத்துக்குடி போல மிகப் புகழ் பெற்ற துறைமுகங்களாகும்!

2. Protocol - நெறி. ஒரு அரசியல் கூட்டம் நடக்கையில் இந்த வார்த்தையைக் கேட்டிருப்போம். அங்கே சரியான நெறிப் - protocol படி நடத்த வேண்டும். முதலில் தலைவர் தான் மேடையேற வேண்டும். அப்புறம் மற்றவர்கள். யார் முதலில் பேசுவது. அப்புறம் கடைசி முடிப்பது எப்படி என்று. அது போலவே இங்கும் பல நெறிகள் உண்டு. உதாரணமாக (http, pop3, smtp, ftp, udp போன்றவை)

3. Application Software - பயன்பாட்டு மென்பொருள். இவை பற்றி அதிகம் சொல்லவேண்டியதில்லை. உங்களுக்கே தெரிந்து இருக்கும். எடுத்துக்காட்டாக (வலை உலாவி, அலுவல் தொகுப்புக்கள், கணக்கீட்டு மென்பொருட்கள்)

4. IP Address - இணைய அடையாள முகவரி - சுருக்கமாக ஐபி முகவரி. இவற்றை எட்டெண்கள் (Octet) ஆகப் பிரித்திருக்கின்றார்கள். ஒரு எட்டெண் என்பது 2^8 ஆகும். அதாவது 0 முதல் 255. இது போல் 4 எட்டெண்கள் கொண்டது ஐபி முகவரி. உதாரணம்: 59.112.34.35 இதன் மூலம் 256 x 256 x 256 x 256 தனிப்பட்ட கணினிகளைச் சுட்ட முடியும்! இதில் நிலை முகவரி (Static IP Address) மாறும் முகவரி (Dynamic IP Address) என்று இரு வகை உண்டு. இது போக முகமூடி வழங்கிகளும் (Proxy Servers) உண்டு!

5. Deny - மறு/ தடை செய்தல்.

6. Allow - அனுமதி

இணையத்தில் ஒரு தகவல் பரிமாற்றம் நடக்கையில் இவை யனைத்தும் சம்பந்தப் படுகின்றன! எனவே தான் தீச்சுவரில் இத்தகவல்களனைத்தும் உபயோகிக்கப் படுகின்றன!

உதாரணமாக நீங்கள் வலையில் உலாவுகின்றீர்கள் என்று வைத்துக் கொள்வோம்: Internet Explorer என்ற பயன்பாட்டு மென்பொருளின் மூலம் http (hypertext transfer protocol) என்ற நெறிப்படி 80 என்ற துறைமுகம் வழியாக யுக்தி முறைமை முகவரியில் இருந்து (logical address எ.கா. http://www.yahoo.com) DNS என்னும் பெயர்க்கள வழங்கி மூலம் அடிப்படை ஐபி முகவரியாக மாற்றப்பட்டு தகவல் பரிமாற்றம் செய்யப்படும்.

எனவே ஒரு தகவல் பரிமாற்றத்தில் துறைமுகம், நெறி, பயன்பாட்டு மென்பொருள், இணைய முகவரிகள் (துவக்கமும் சேருமிடமும்) ஆகியவையும் தகவலுடன் சேர்ந்து செல்கின்றன. இவற்றில் சில தொடர்புடையவையும் ஆகும்! உதாரணமாக http சாதாரணமாக 80 அல்லது 8080 என்ற துறைமுகம் மூலமாகவே அனுப்பப்படும். அதற்காக மற்ற துறைமுகங்களில் அனுப்பப்படக் கூடாது என்று அர்த்தம் இல்லை. மற்ற துறைமுகங்கள் மூலமும் அனுப்பலாம். அப்படி அனுப்பும் போது அவற்றை உலாவி எடுத்துக் கொள்ளாது. இதுவே நச்சுப் பொருட்கள் அனுப்புவோர் உபயோகித்துக் கொள்கின்றனர். மொத்தம் 65535 துறைமுகங்கள்

இருக்கின்றன!

தீச்சுவரில் எவ்வாறு தடுப்பது?

இந்த நான்கின் மூலமாகவோ, இவற்றை இணைப்பதன் மூலமோ சில விதிகளைச் செய்வதன் மூலம் நச்சுப் பொருட்கள் வருவதைத் தவிர்க்க இயலும்.

1. **ஐபி முகவரி முறை**: இந்த முறையில் ஐபி முகவரியைக் கொண்டு தடை செய்யவோ, அனுமதிக்கவோ செய்யலாம். உதாரணமாக 59.* என்று வரும் ஐபி முகவரியைத் தடை செய்க எனலாம். அல்லது 59.* இது மட்டுமே அனுமதிக்கப்பட்ட ஐபி எனலாம்! அப்படிச் சொல்லி விட்டால் அந்த முகவரி தவிர வேறெங்கிருந்து வந்தாலும் தீச்சுவர் உள்ளே விடாது!

2. **பயன்பாட்டு மென்பொருள் முறை**: இந்த முறையில் ஒரு குறிப்பிட்ட மென்பொருள் இணையத்தைத் தொடர்பு கொள்வதைத் தவிர்க்கவோ அல்லது அனுமதிக்கவோ செய்யலாம். உதாரணமாக, உங்கள் பிணையத்திலிருந்து மின்னஞ்சலே அனுப்பக் கூடாது என்றால் மின்னஞ்சல் அனுப்பும் மென்பொருட்களைத் தடை செய்யலாம். அல்லது உலாவி மென்பொருட்களை மட்டுமே அனுமதிக்கலாம்!

3. **துறைமுக முறை**: இதன் மூலம் நீங்கள் குறிப்பிட்ட துறைமுகத்திலிருந்து வரும் தகவல்களை அனுமதிக்கவோ அல்லது மறுக்கவோ முடியும். உதாரணமாக 21 என்ற துறைமுகத்தை அடைத்து விட்டால் ftp மூலம் வரும் கோப்புக்களைப் பகிர்ந்து கொள்ள முடியாது.

4. **நெறி முறை**: இந்த முறை மூலம் குறிப்பிட்ட நெறி மூலம் வரும் தகவலை அனுமதிக்கவோ மறுக்கவோ முடியும். உதாரணமாக http நெறியை அடைத்து விட்டால் யாருமே உலாவியில் உலாவ முடியாது. அது எந்த மென்பொருளாய் இருந்தாலும் சரி.

இவையனைத்தும் உட்புகும் தகவல்கள் அல்லது வெளிச்செல்லும் (Inward/outward) என்று இரண்டு வகையாய் விதிகளை அமைக்கலாம்.

அனுமதித்தல் மறுத்தல் இரண்டினையும் அறிந்து கொள்தல் அவசியமாகும். ஒன்றினை அனுமதி என்றால் மற்ற அனைத்தும் தடையா? என்பதையும், ஒன்றை மறுத்தால் மற்ற அனைத்துக்கும் அனுமதி உண்டா என்பதையும் ஞாபகம் வைத்துக் கொள்ள வேண்டும்.

நீங்கள் அடிக்கடி இணையத்தில் உலவுபவர் என்றால் 80 தவிர மற்ற துறைமுகங்களை அடைத்து விடலாம். இனி 80 வழியாக http நெறி மூலம் மட்டுமே தகவல் பரிமாறிக் கொள்ளலாம் என்று விதிக்கலாம். இதையும் தாண்டி வரும் நச்சுக்களை வேறெதுவும் மென்பொருளை உபயோகிக்க முடியாமல் செய்வதன் மூலமும், இணைய முகவரியைக் கண்டறிவதன் மூலமும் அறிந்து கொள்ளலாம்.

தீச்சுவர் சரியான பாதுகாவலனாகவும் இருக்காமல், பதிகை (log) மூலம் அனைத்து நிகழ்வுகளையும் பதிந்து வைத்திருப்பதால் எந்த நேரம் யார் யாரிடம் எந்த மென்பொருள் மூலம், எந்த துறைமுகத்தில் எந்த நெறியின் மூலம் தொடர்பு கொண்டார்கள், எத்தனை பொட்டலங்கள் பகிர்ந்து கொண்டனர் போன்ற தகவல்களைப் பெற முடியும்!

சரி. http மூலமாகவே, 80 என்ற துறைமுகம் மூலமாகவே, internet explorer ஐத் தாக்குவதாகவே, நம்பத்தகுந்த இணைய முகவரியில் இருந்து வந்தால் என்ன செய்வது? சரியான அடையாள அட்டையைக் கொண்டு வரும் கொலைகாரனை உள்ளே காவலாளி விடும் கதை தான் இங்கேயும்.

அதற்கு விடை இந்த இடத்தில் தான் ஒற்றுக் காணும் மென்பொருட்கள், வைரசு கண்டு பிடிக்கும் ஆண்டி வைரசு மென்பொருட்கள் ஆகியன உபயோகிக்கப்பட வேண்டும். வெறுமனே தீச்சுவர் மட்டுமே போதாது. ஆனால் சரியான தீச்சுவர் விதிகள் செயல்படுத்தப்பட்டு இருந்தாலே மிகப் பெரும்பான்மையான பிரச்னைகள் முளையிலேயே கிள்ளி எறியப்படும்.

மேலும் நிறைய தீச்சுவர்கள் நிறுவுவதால் பயனேதும் இருக்கப் போவதில்லை. இரு தீச்சுவர்களும் சண்டை போட்டு கடைசியில் நச்சுப் பொருள் உள்ளே நுழைந்து விடும் வாய்ப்பு இருக்கின்றது! எனவே மிகச்

சரியான விதிமுறைகளைக் கடைப்பிடித்து தீச்சுவர்களைச் சரியாகப் பயன்படுத்தி பாதுகாப்பாக இணையத்தினை அனுபவிப்போம் என்று முடிவெடுப்போம். நன்றி.