# एक परिचारक के लिए आयपीटेबल संग फायरवाल

फायरवाल आगमन यातायात को छलनी कर उन सभी कंप्यूटर की रक्षा करती है ज्यो इंटरनेट से जुड़े होते है। हर वरकस्टेशन और सरवर पर फायरवाल होनी ही चाहिए यद्यपि वह कंपनी अपने आंतरिक नेटवर्क और इंटरनेट के बीच फायरवाल रखती है। यह परलेख साद्यारण आयपीटेबल फायरवाल पर आद्यारित है।



## क्यों यह फायरवाल

आयपीटेबल बड़ी फायरवाल के लिए बहखुबी समायोजन करता है। यहां तक की कइ यांत्रिक फायरवाल भी आयपीटेबल, या उसकी पूर्ववर्ती आयपीचैन, का उपयोग करतीं हैं। क्योंकी कइे लनिक्स वतिरणों पर आयपीटेबल आरम्भ से संस्थापित होती हैं, आप तुरंत उनका उपयोग शुरु कर सक्ते हैं। हालॉकी आयपीटेबल के लिए कई आरेखीय प्रयोक्ता अंतरानीक उपलब्ध है, पर वह बहुत निम्नस्तर के हैं। नमुने के लिए लोककिट, रेड हेट का उपलब्ध उपकरण, जो आयपीटेबल को रूप देने में उपयोग किया जाता हैं, यह नहीं दिखाता की उपयोक्ता ने पूर्व किन नयिमों का उपयोग किया, हाथ से किये गय बदलाव के ऊपर लिखना और बहुत खतरनाक और व्यर्थ विकल्प, बिना किसी मदद के प्रस्तुत करता हैं।

आगे दी हुई शैल स्क्रिप्ट फायरवाल की रूपरचना तैयार व भंडारण करती हैं ताकी जब कभी कंप्यूटर बूट हो, वह स्वतः शुरु हो जाय। यदि आप फायरवाल का रूपांतर करना चाहते हैं, बस स्क्रिप्ट का संपादन कर उसे दोबारा रन करें। फायरवाल को संस्थापन करने का उचित समय तब होता हैं जब कंप्यूटर पहली बार नेटवर्क से जोडा जाता हैं।

su – आदेश देकर पहले मूल उपयोगकरता बने। नीचे दी गइ स्क्रिप्ट को इस पते पर भंडारण करे /root/bin/firewall.sh

```
#!/bin/sh
# firewall.sh - Configurable per-host firewall for workstations and
# servers.(c) 2003 Tero Karvinen - tero karvinen at iki fi - GPL
# Cleanup old rules # All the time firewall is in a secure, closed state
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables --flush       # Flush all rules, but keep policies
iptables --delete-chain
## Workstation Minimal firewall ###
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -A INPUT -i lo --source 127.0.0.1 --destination 127.0.0.1 -j ACCEPT
iptables -A INPUT -m state --state "ESTABLISHED,RELATED" -j ACCEPT
```

```
iptables -A INPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
iptables -A INPUT -p icmp --icmp-type time-exceeded -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
####### HOLES ####### Edit holes below, then run this script again
#iptables -A INPUT -p tcp --dport ssh -j ACCEPT
#iptables -A INPUT -p tcp --dport http -j ACCEPT
#iptables -A INPUT -p tcp --dport https -j ACCEPT
###################### Edit above
iptables -A INPUT -j LOG -m limit --limit 40/minute
iptables -A INPUT -j DROP
# Save
iptables-save > /etc/sysconfig/iptables
echo ": Done."
```

अब अनुकूलन संस्थापित करने के लिए, इस स्क्रिप्ट को रन करें

```
# chmod u+x /root/bin/firewall.sh
# /root/bin/firewall.sh
```

इसे कहना चाहिए "firewall.sh: Done"। आप अपना अनुकूलन iptables –L से जॉच सक्ते हैं।

भहुत अच्छे, अब आपके पास एक फायरवाल हैं।

आयपीटेबल और नेट के साथ आप इंटरनेट कनेकशन बांट भी सक्ते हैं।

# Adminstrivia

Tested with Red Hat Linux 9 Shrike.

Changelog:

- 2006-08-18 Copywriting document. Linked to Johansens' (2006) init.d version.
- 2003-11-19 Separated nat to its own document
- Earlier ChangleLog missing.



Translated by : Amrit Bansal