

VMware administration



Innehåll

WMware installation och administration

Nätverkssäkerhet

NAT, SAT

IP-tables

Installation av Esxi 5.0

Hårdvarukrav

- »CPU: 2x2GHz
- »Minne: 6GByte
- »Nätverkskort: 2st.

Starta vSphereClient och logga in
Montera ISO-fil och kör!
Notera root-lösenord



De olika flikarna

Getting Started: Start/Stopp samt inställningar

Summary: Info om virtuell maskin

Resource

Allocation: Allokerade resurser

Performance: Resursutnyttjande

Events: Händelselogg

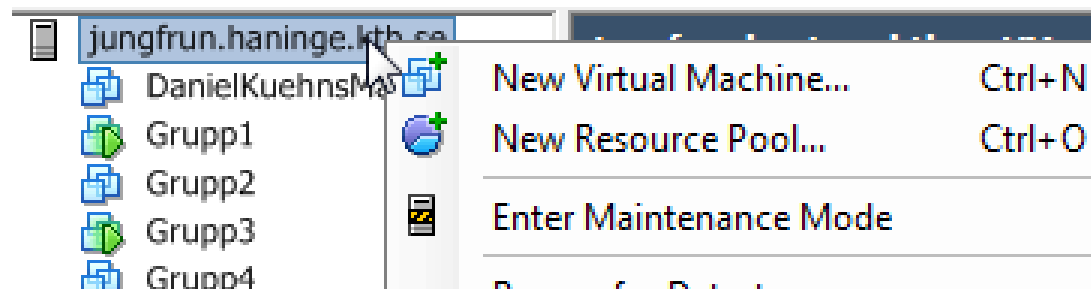
Console: Konsol

Permissions: Rättighetstilldelning

Skapa virtuella maskiner

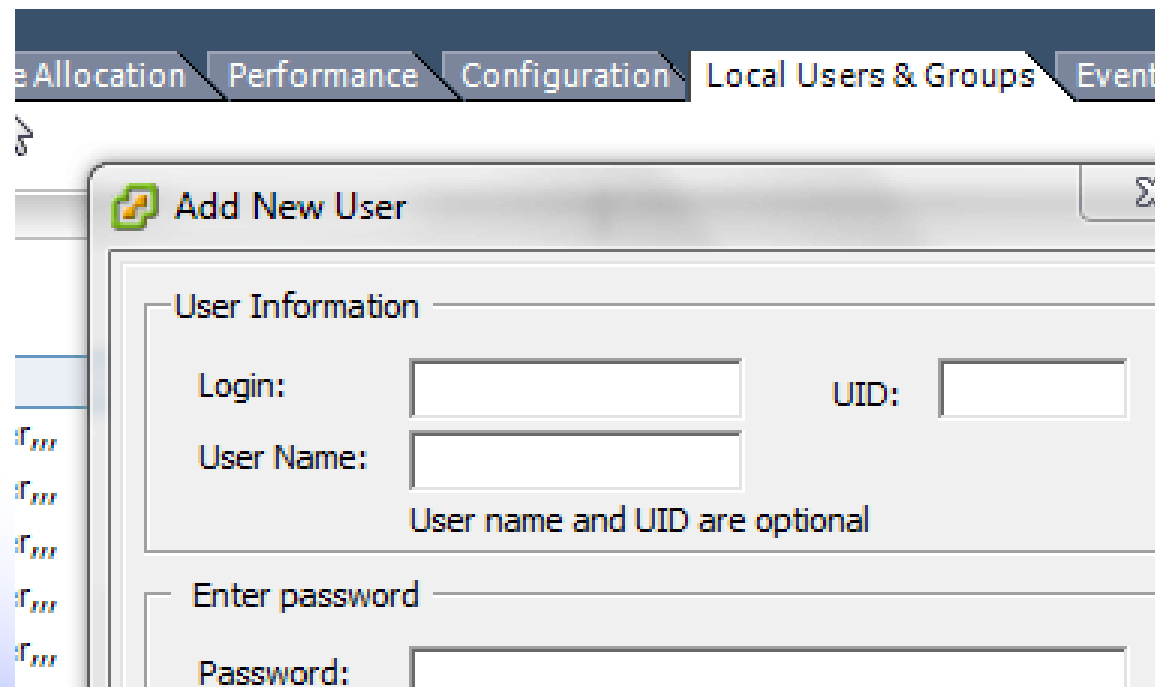
Högerklicka på servern och välj.

Ctrl+N snabbkommando



Skapa användare

Flik "Local Users & Groups"
Högerklicka och välj

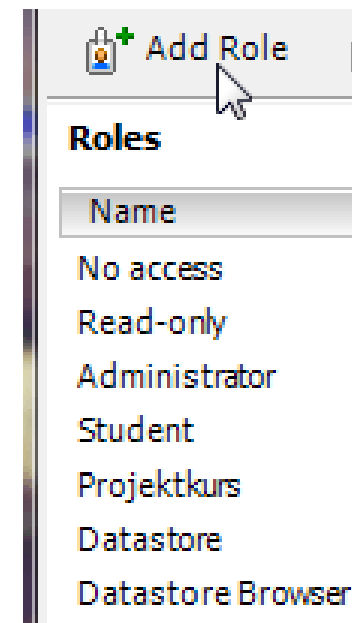


The screenshot shows a software interface with a tabbed menu at the top. The tabs are: "Allocation", "Performance", "Configuration", "Local Users & Groups" (which is selected), and "Event". Below the tabs, a dialog box titled "Add New User" is open. The dialog box has a "User Information" section with the following fields: "Login:" with an input box, "UID:" with an input box, and "User Name:" with an input box. Below these fields, a note states "User name and UID are optional". There is also an "Enter password" section with a "Password:" label and an input box. The dialog box has a green icon with a plus sign in the top-left corner and a close button (X) in the top-right corner.

Skapa Role (profil)

Home – Administration – Roles

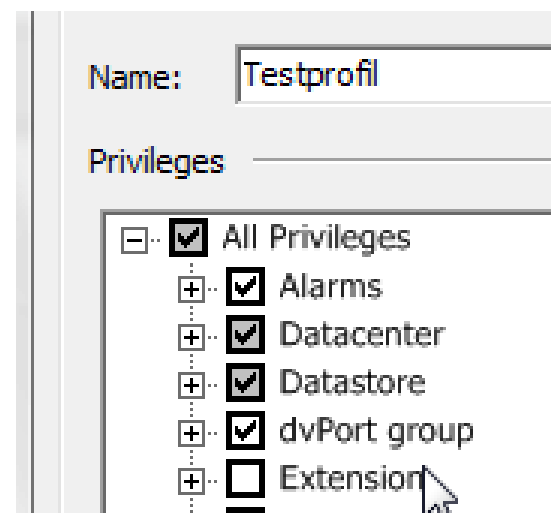
Add Role



Namnge och sätt rättigheter

Välj rättigheter som ska tillhöra profilen.

Gråmarkerade rutor indikerar att underliggande rättigheter ej är fullständiga.



The screenshot shows a configuration window for a user profile. At the top, there is a text field labeled 'Name:' containing the text 'Testprofil'. Below this is a section titled 'Privileges'. Under the 'Privileges' section, there is a list of privilege categories, each with a checkbox and a plus icon to its left. The categories are: 'All Privileges' (checked), 'Alarms' (checked), 'Datacenter' (checked), 'Datastore' (checked), 'dvPort group' (checked), and 'Extension' (unchecked). A mouse cursor is pointing at the 'Extension' checkbox.

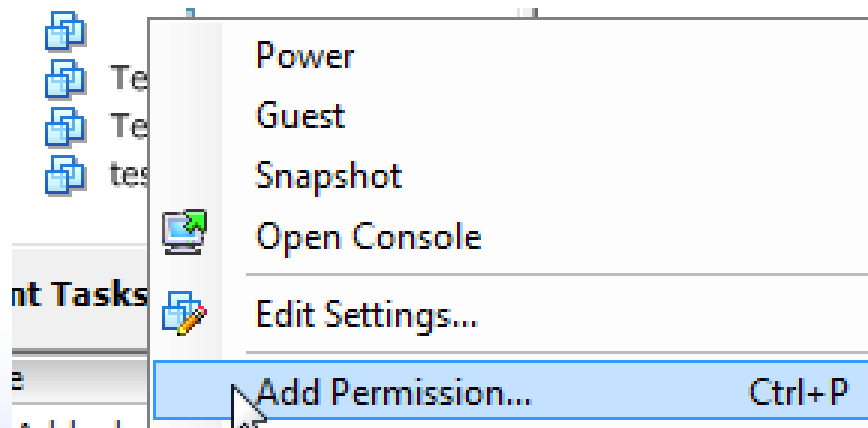
Privilege Category	Selected
All Privileges	Yes
Alarms	Yes
Datacenter	Yes
Datastore	Yes
dvPort group	Yes
Extension	No

Dela ut rättigheter till användare

Markera server,

Högerklicka och välj Add Permission


Snabbkommando: Ctrl+P



Dela ut rättigheter till användare

Välj användare som ska tilldelas rättigheter och därefter passande Role.

Ska rättigheterna ärvas nedåt eller ej?

Name	Role	Propagate
 mll-test	Testprofil	Yes

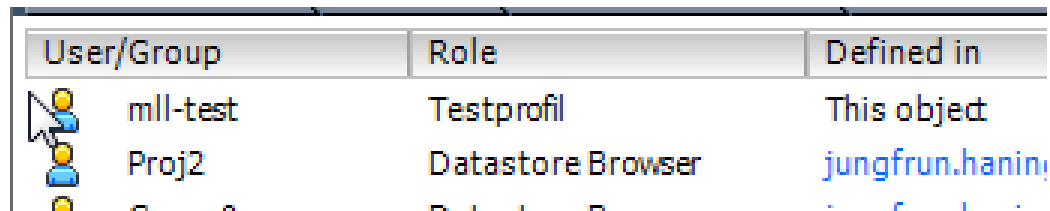
Testprofil

- ☒ All Privileges
 - ☒ Alarms
 - ☒ Datacenter
 - ☒ Datastore




☒ Propagate to Child Objects

Verifiera rättighetstilldelningen

Under flik "Permissions" kan rättighetstilldelningen verifieras.



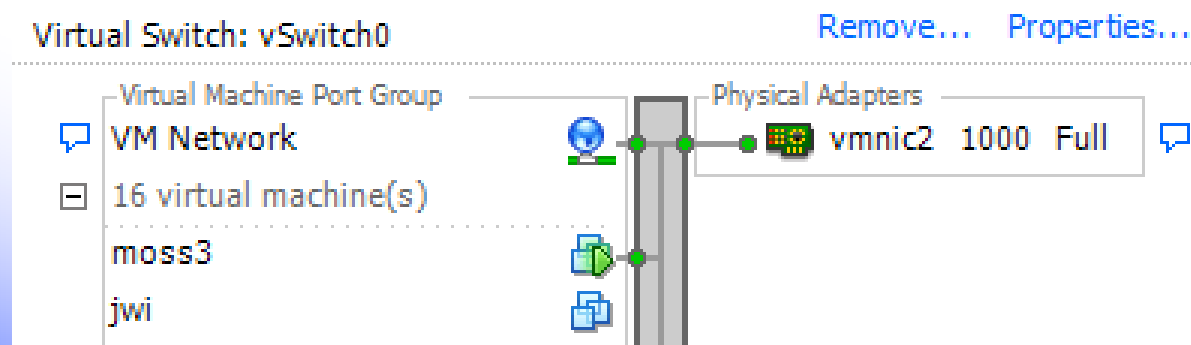
A screenshot of a permissions table from a software application. The table has three columns: 'User/Group', 'Role', and 'Defined in'. The first row shows a user icon, 'mll-test', 'Testprofil', and 'This object'. The second row shows a user icon, 'Proj2', 'Datastore Browser', and a blue hyperlink 'jungfrun.hanin...'. The third row is partially visible with a user icon and the text 'Datastore Browser'.

User/Group	Role	Defined in
 mll-test	Testprofil	This object
 Proj2	Datastore Browser	jungfrun.hanin...
	Datastore Browser	...

Virtuella switchar




Markera ESXi servern och klicka på fliken "Configuration". Samt välj "Networking".
En lista med befintliga nät kommer att visas.

View: Virtual Switch
Networking



Virtuella switchar

Välj "Add Networking" – "Connection type, Virtual machine" och därefter "Create a virtual switch".

<input checked="" type="radio"/> Create a virtual switch	Speed	Networks
<input type="radio"/> Use vSwitch0	Speed	Networks
<input type="checkbox"/>  vmnic2	1000 Full	130.237.80.1-13
<input type="radio"/> Use vSwitch1	Speed	Networks
<input type="checkbox"/>  vmnic5	1000 Full	172.17.83.128-1
<input type="checkbox"/>  vmnic4	1000 Full	172.17.83.128-1










Virtuella switchar

Namnge det virtuella nätverket samt slutför processen. En ny virtuell switch har skapats ansluten till det nya virtuella nätet.

Nu återstår bara att ansluta virtuella maskiner till switchen.

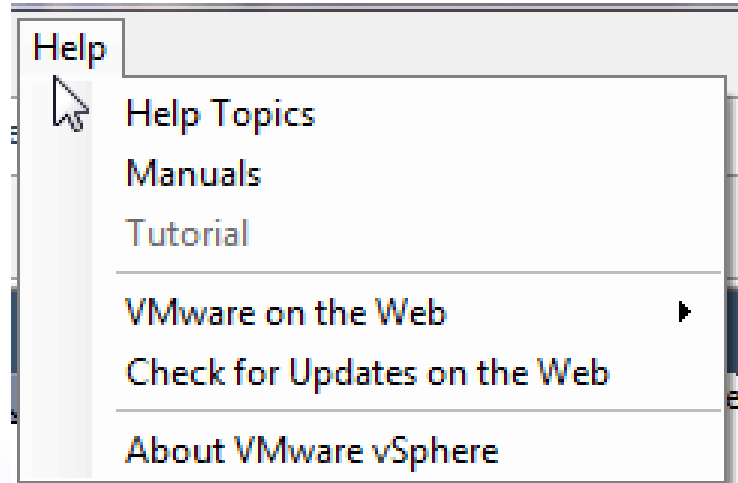
Anslut maskiner

Högerklicka på vald maskin och välj "Edit settings". Anslut därefter nätverkskortet till rätt virtuellt nät.

Hardware	Summary
 Memory	256 MB
 CPUs	1
 Video card	Video card
 VMCI device	Restricted
 SCSI controller 0	LSI Logic Parallel
 Hard disk 1	Virtual Disk
 CD/DVD Drive 1	Client Device
 Network adapter 1	VM Network
 Floppy drive 1	Client Device

Hjälpfunktion

VMware har även en utmärkt inbyggd hjälpfunktion som kan lösa många knutar.



Nätverkssäkerhet

Inloggningssäkerhet

- » Namnkonventioner, Lösenord
- » Inloggningsmöjligheter

Rättigheter/Behörigheter

Kryptering, Certifikathantering

Nätverksimplementering

Brandväggslösningar

- » Olika typer av brandvägg
- » Konfiguration av brandvägg.

Brandväggar

Kopplas in mellan det lokala systemet och Internet för att uppnå acceptabel säkerhetsnivå.

I allmänhet en router eller dator med två nätverkskort som endast släpper igenom vissa typer av trafik.

Vilket typ av trafik som släpps igenom bestäms av brandväggens s.k. filter-regler.

Fiilterregler

Reglerna sparas i en tabell, eller lista

» Access Control List (ACL)

Reglerna behandlas uppifrån och neråt.

» När en regel matchas utförs regeln och exekveringen

Action	Source	Src port	Dst	Dst port	flags
Allow	Our net	>1023	*	80	*
Allow	*	80	Our net	>1023	ACK
Deny	*	*	*	*	*

Filtrerade tjänster

Exempel på vanliga tjänster som kan filtreras:

- »SMTP (E-mail)
- »TELNET (Terminalemulering)
- »FTP (Filöverföring)
- »FINGER (Användarinformation)
- »NFS (Fildelning, distribuerade filsystem)

Brandväggar

Brandväggar möjliggör blockering av en tjänst i båda riktningarna, eller endast i ena.

Portnummer används för att ange vilken tjänst som skall filtreras.

Brandväggar underlättar administrationen av säkerheten.

Loggning av kritiska funktioner.

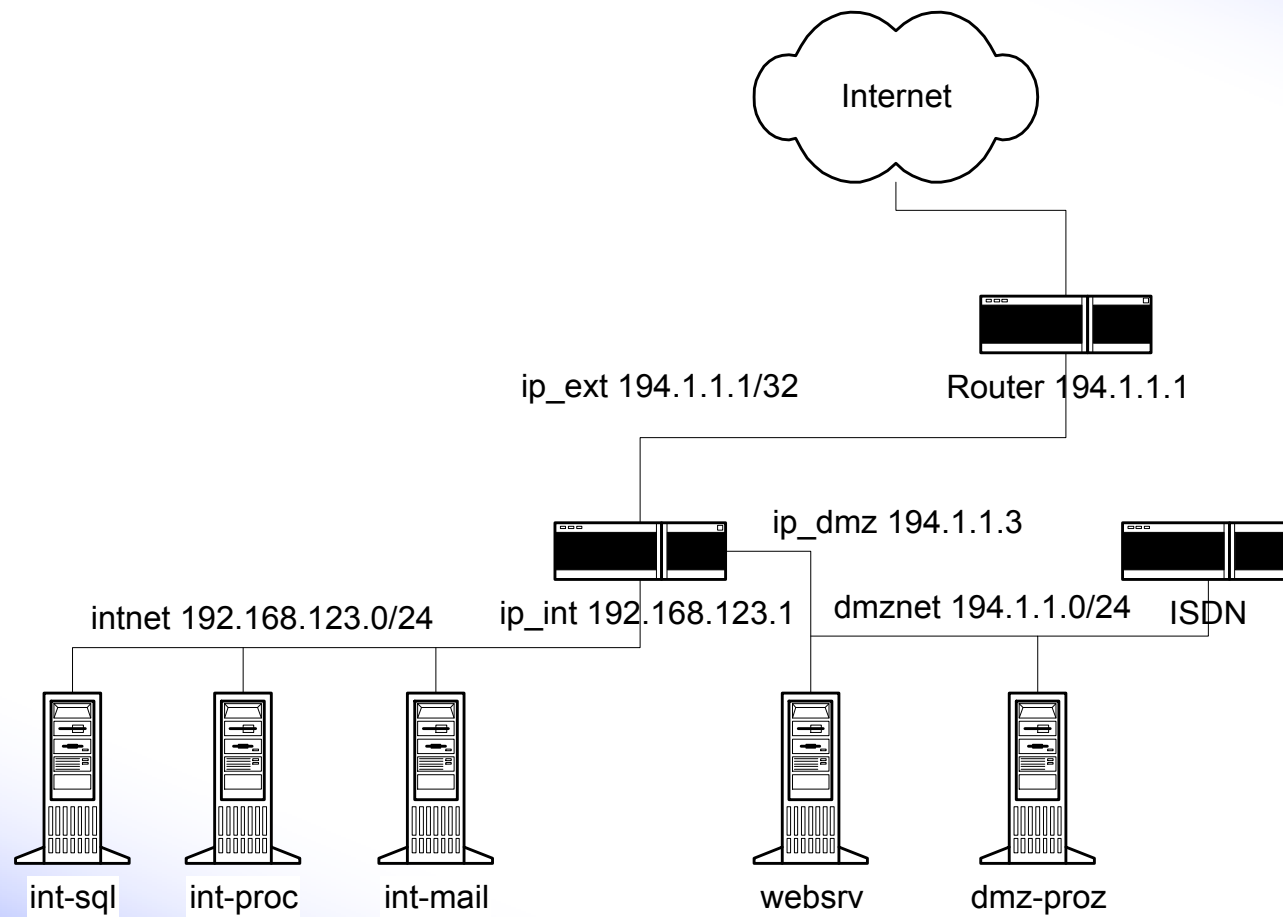
DMZ (Demilitarized Zone)

Skyddat nät mellan externa och interna nätet.

Ansluter mot brandvägg med separat NIC.

Används om man vill göra egna servrar publikt åtkomliga, men samtidigt skyddade.

Exempel på brandväggslösning



Brandväggar

En brandvägg skyddar mot:

- »Otlillåten trafik enligt konfiguration.

- »*Ex. HTTP släpps igenom men FTP spärras.*

En brandvägg skyddar inte mot:

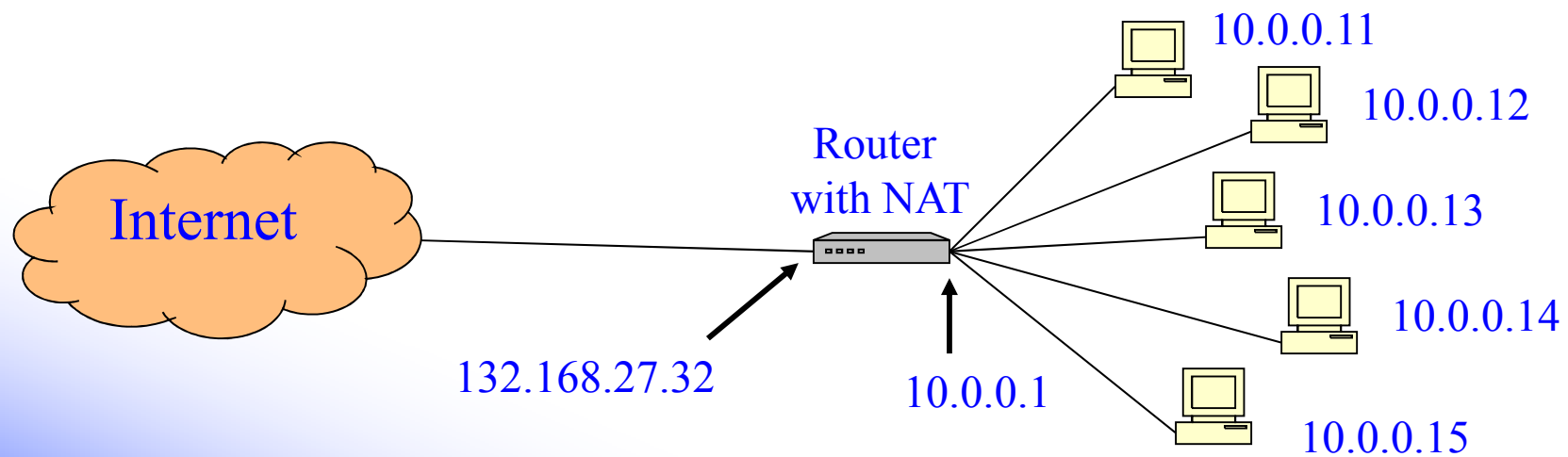
- »Virusangrepp

- »Dåligt genomtänkt säkerhetsstrategi

En vanlig brandvägg kan endast tolka IP, TCP, UDP och ICMP, men inte applikationsprotokoll.

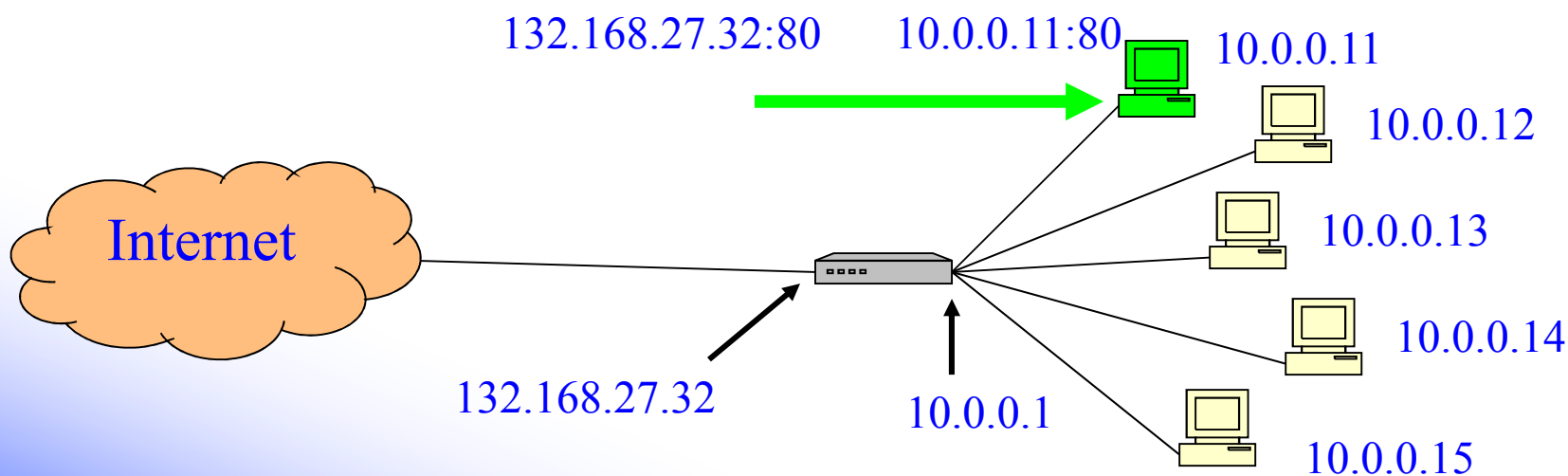
NAT (Network Address Translation)

- » Översätter interna IP-adresser och portnummer
- » Kan implementeras i de flesta routrar, OS.
- » Döljer privat nät från publikt nät.
- » All utgående trafik ser ut att komma från en enskild adress, routerns externa



Port Forwarding (SPAT, SNAT)

Port Forwarding tillåter router/brandvägg att publicera en eller flera IP-adresser på externa infacet.



Port-mappad NAT (NAPT)

NAT arbetar med block av portnr.

»Varje intern PC tilldelas ett NAT portnummer när den ansluter mot en extern adress

Privat adress	Privat port	Extern adress	Extern port	NAT port	Använt protokoll
10.0.0.5	21023	128.10.19.20	80	14003	TCP
10.0.0.1	3862	128.10.19.20	80	14010	TCP
10.0.2.1	26600	207.200.75.200	21	14012	TCP
10.0.0.3	1274	128.210.1.5	80	14007	TCP

IP-tables

Paketfiltrerande brandvägg som är förinstallerad i Ubuntu

- »All trafik tillåts default
- »Regler saknas, måste skapas

- »Lista IP-tables regler

- »`sudo ip-tables -L`

Tre regellistor

INPUT

- »Behandlar inkommande trafik

FORWARD

- »Trafik genom brandvägg till målnät

OUTPUT

- »Behandlar utgående trafik

Turordning i listorna

Trafik matchas mot reglerna i listorna steg för steg uppifrån och ned

Vid träff utförs regeln och listan lämnas

- »target = LOG, lämnar EJ listan

- »Ev. DROP ALL regel längs ned på listan

Två strategier

Accept specified

Deny all

Deny specified

Accept all

Den första är att föredra!

Varför?

Iptables Syntax

```
Iptables -F chain-name
```

```
Iptables -P chain-name target
```

```
Iptables -A chain-name -i interface -j target
```

» -F (Flush) Rensar tidigare regler i lista

» -P (Policy) Anger default policy för lista

» -A (Append) Lägg till regel i lista

»target (ACCEPT, REJECT, DROP, LOG)

Tillåt etablerade sessioner

```
sudo iptables -A INPUT -m state --state  
ESTABLISHED,RELATED -j ACCEPT
```

- » -A INPUT: Gäller inkommande trafik
- » -m state: matcha förbindelsens status
- » --state: ESTABLISHED, RELATED
 - » *Är förbindelsen etablerad*
- » -j ACCEPT: Vid träff, acceptera paketet

Tillåt inkommande ssh-trafik

```
sudo iptables -A INPUT -p tcp --dport 22  
-j ACCEPT
```

- » -A INPUT: Gäller inkommande trafik
- » -p tcp: undersöker om det är TCP-trafik
- » --dport 22: undersöker om port 22 avses
- » -j ACCEPT: Vid träff, acceptera paketet

Tillåt inkommande webbtrafik

```
sudo iptables -A INPUT -p tcp --dport 80  
-j ACCEPT
```

- » -A INPUT: Gäller inkommande trafik
- » -p tcp: undersöker om det är TCP-trafik
- » --dport 80: undersöker om port 80 avses
- » -j ACCEPT: Vid träff, acceptera paketet

Blockera all övrig trafik

```
sudo iptables -A INPUT -i eth0 -j DROP
```

- » -A INPUT: Gäller inkommande trafik
- » -i eth0: Gäller endast interface eth0
- » -j DROP: Droppa all trafik

Lista och spara reglerna

Lista regler som skrivits in
»`sudo iptables -L`

Spara godkänd lista
»`iptables-save`

Firewall Builder

Firewall Builder: test.fwb, rev 1.9

Firewalls: test

Policy | outside | inside | loopback | NAT

	Source	Destination	Service	Action	Time	Options	Comment
0	net-192.168.1.0	test	ssh	Accept	Any		SSH Access to firewall is permitted only from internal network
1	test	net-192.168.1.0	DNS	Accept	Any		Firewall uses one of the machines on internal network for DNS
2	Any	test	Any	Deny	Any		All other attempts to connect to the firewall are denied and logged
3	net-192.168.1.0	Any	Any	Accept	Any		
4	Any	loopback	Any	Deny	Any		
5	loopback	Any	Any	Deny	Any		

Object Type: Firewall
Object Name: test
Platform: iptables
Version:
Host OS: linux24

This firewall has two interfaces. Eth0 faces outside and has a dynamic address; eth1 faces inside. Policy includes basic rules to permit unrestricted outbound access and anti-spoofing rules. Access to the firewall is permitted only from

www.versiontracker.com