

Project G-Cloud Setup

Name	value
Project	SAWFT
Project ID	sawft-275017
Cloudguard Admin User	admin
Cloudguard Admin PW	MesvQPH5h95c
Cloudguard internalIP(default)	10.128.0.2
Cloudguard internalIP(my-vpc)	192.168.23.2
Cloudguard externalIP	34.71.14.71

Lab 1.1: Connecting to Management

Um via Gaia Interface eine Verbindung aufbauen zu koennen war eine zusaetzliche Firewall Regel notwendig, welche den Traffic zur Firewall frei gibt.

Fingerprint der Cloudguard:

```
THIN LEAD AWN LYE MAST MOLE ROUT AUK ARGO GALT CAL BLEW
```

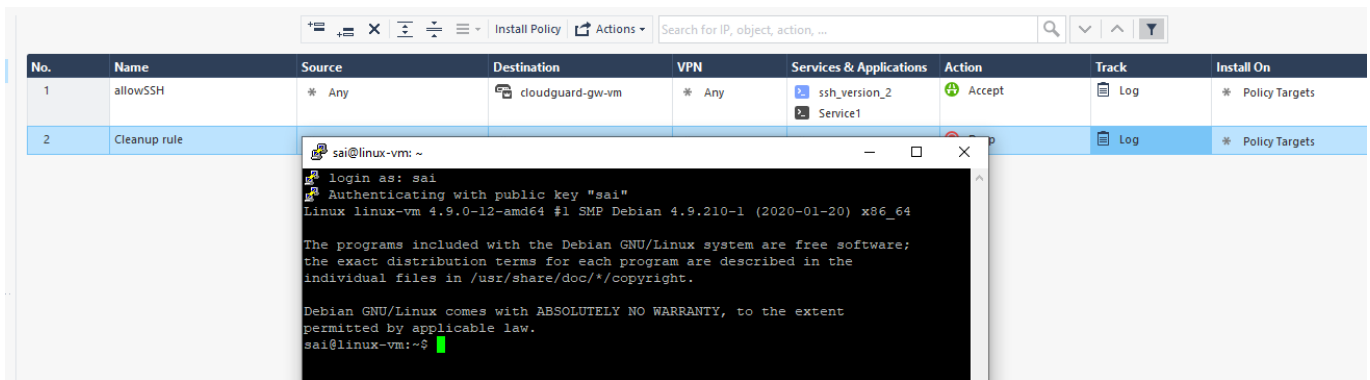
Der Fingerprint dient zur Identifikation der verbundenen Appliance. Jedes device hat im Normalfall einen eigenen Fingerprint. So kann ein Vergleich zwar keinen Man-In-The-Middle-Angriff nicht verhindern aber erkennen. Im einfachen Falle kann so auch einfach ueberprueft werden ob man sich mit der gewuenschten Appliance verbunden hat.

Lab 1.2: SSH Connection to Linux Instance

Angelegte Regeln mit den verwendeten Objekten.

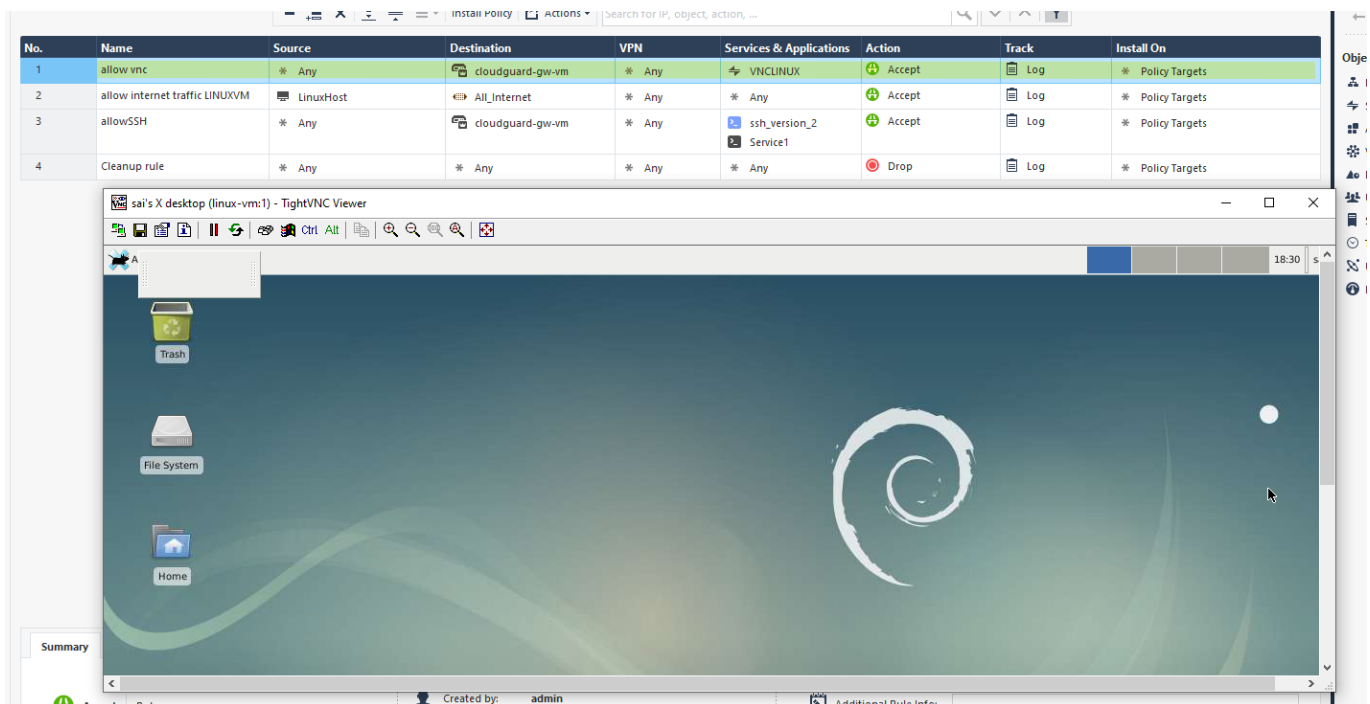
No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On	Comments
1	* Any	cloudguard-gw-	Service1	= Original	LinuxHost	ssh_version_2	cloudguard-gw...	
Automatic Generated Rules : Machine Static NAT (No Rules)								
Automatic Generated Rules : Machine Hide NAT (No Rules)								

Erfolgreiche Verbindung via SSH und Key-Authentication zur Linux VM



Lab 1.3: VNCServer & NAT Rules

- Regel erstellt um von LinuxVM ins internet zugreifen zu koennen.
- Schritte aus Labanweisung durchgefuehrt.
- NAT Regel Inbound von Port 3332 auf LinuxVM:5901. Es werden 2 Serviceobjekte fuer die NAT-Regel benoetigt.
- Security Policy welche den VNC custom Port (Service Objekt) Inbound auf die LinuxVM erlaubt



Fragen 1: Application Control & URL Filtering

Fallstrick: Es muss noch das Applicationfiltering in den Policies Enabled werden um die Liste mit den Services auswaehlen zu koennen.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	block facebook	* Any	* Any	* Any	Facebook Facebook Messenger	Drop	None	* Policy Targets
2	allow vnc	* Any	cloudguard-gw-vm	* Any	VNCLINUX	Accept	Log	* Policy Targets
3	allow internet traffic LINUXVM	LinuxHost	All_Internet	* Any	* Any	Accept	Log	* Policy Targets
4	allowSSH	* Any	cloudguard-gw-vm	* Any	ssh_version_2 Service1	Accept	Log	* Policy Targets
5	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

Summary

Details

Drop

Rule 1

block facebook

sai's X desktop (linux-vm:1) - TightVNC Viewer

www.facebook.com - Chromium

New Tab - Chromium

www.facebook.com

Search Google or type a URL

h.org Latest News Help

Gmail Images

This site can't be reached

The connection was reset.

Try:

Checking the connection

Checking the proxy and the firewall

ERR_CONNECTION_RESET

Die Applikation Security Policy wirkt bei HTTP aber nicht bei HTTPS.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	block google service	* Any	* Any	* Any	Google Maps	Drop	None	* Policy Targets
2	block facebook	* Any	* Any	* Any	Facebook Facebook Messenger	Drop	None	* Policy Targets
3	allow vnc	* Any	cloudguard-gw-vm	* Any	VNCLINUX	Accept	Log	* Policy Targets
4	allow internet traffic LINUXVM	LinuxHost	All_Internet	* Any	* Any	Accept	Log	* Policy Targets
5	allowSSH	* Any	cloudguard-gw-vm	* Any	ssh_version_2 Service1	Accept	Log	* Policy Targets
6	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

Summary

Details

Drop

Rule 1

block google service

sai's X desktop (linux-vm:1) - TightVNC Viewer

maps.google.com - Chromium

Google Maps - Chromium

maps.google.com

https://www.google.com/maps/@37.6,-95.665,4z

Search Google Maps

See travel times, traffic and nearby places

Sign in

This site can't be reached

The connection was reset.

Try:

Checking the connection

Checking the proxy and the firewall

ERR_CONNECTION_RESET

Date created: 5/13/2020 12:00 PM

Ticket Number: