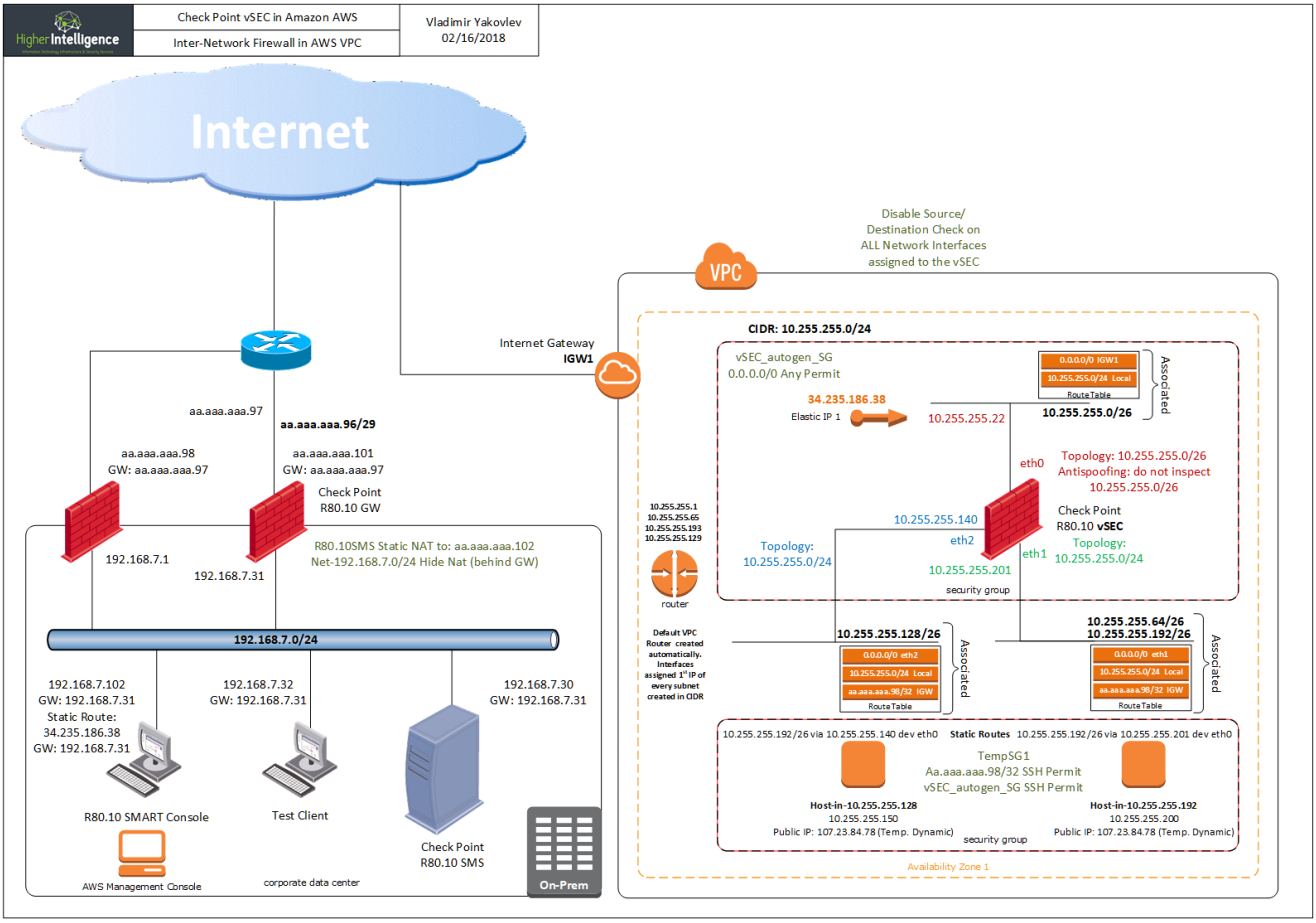
Inspection of Inter-Subnet traffic in AWS VPC using CloudGuard

I've been asked an interesting and, seemingly, trivial question: "How would you protect the hosts in AWS VPC located in a different subnets by inspecting traffic between them?"

I was also assured that presently, AWS did not have a solution to this problem, as every routing table you create will contain "local" route, all traffic from all subnets within one VPC will be routed through it.

To work on this puzzle, this lab environment was provisioned:



...and answer to this dilemma is to use static routes <u>in the instances</u> pointing to the interfaces of the vSEC or cluster, as well as security groups as Sources fro the traffic to the Private Subnets:

[root@ip-10-255-255-200 ec2-user]# route

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.255.255.193  0.0.0.0         UG    0      0        0 eth0
10.255.255.128  10.255.255.201  255.255.255.192 UG    0      0        0 eth0
10.255.255.192  *               255.255.255.192 U     0      0        0 eth0
169.254.169.254 *               255.255.255.255 UH    0      0        0 eth0
[root@ip-10-255-255-200 ec2-user]#
```

```
[root@ip-10-255-255-150 ec2-user]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.255.255.129  0.0.0.0         UG    0      0        0 eth0
10.255.255.128  *               255.255.255.192 U     0      0        0 eth0
10.255.255.192  10.255.255.140  255.255.255.192 UG    0      0        0 eth0
169.254.169.254 *               255.255.255.255 UH    0      0        0 eth0
[root@ip-10-255-255-150 ec2-user]#
```

With Firewall Access rules set:

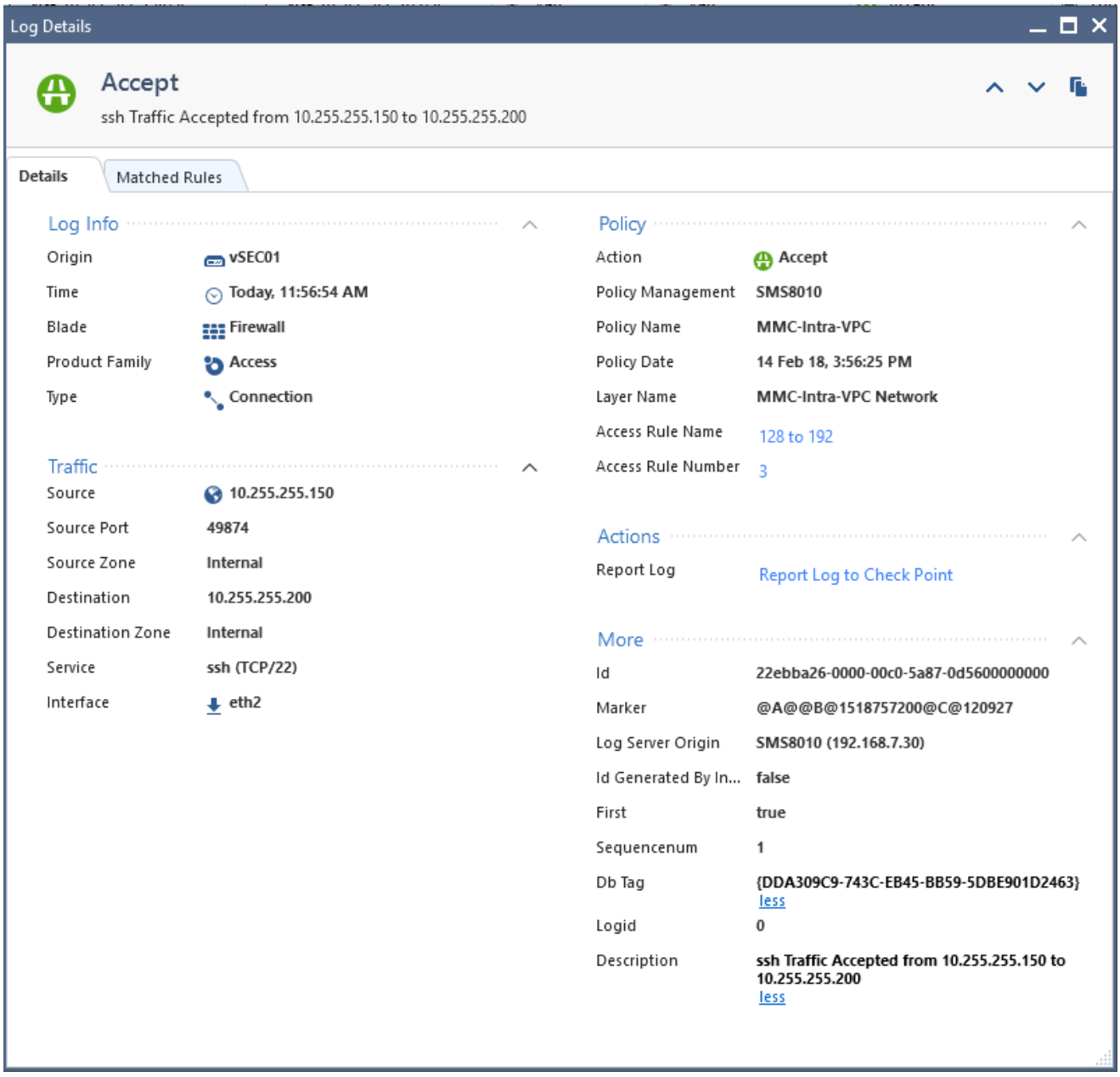
No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	Management-to-vSEC01	Drawbridge	vSEC01	Any	Any	Accept	Log	vSEC01
2	Net_10.255.255.192 Web Access	Net-10.255.255.192/26	Any	Any	http https	Accept	Log	vSEC01
3	128 to 192	Net-10.255.255.128/26	Net-10.255.255.192/26	Any	Any	Accept	Log	vSEC01
4	192 to 128	Net-10.255.255.192/26	Net-10.255.255.128/26	Any	Any	Accept	Log	vSEC01
5	Cleanup rule	Any	Any	Any	Any	Drop	Log	vSEC01

Missing cleanup rule - Unmatched traffic will be dropped and not logged.

With NAT rules set to:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On	Comments
1	Net-10.255.255.192/26	Net-10.255.255.128/26	Any	Original	Original	Original	Policy Targets	
2	Net-10.255.255.128/26	Net-10.255.255.192/26	Any	Original	Original	Original	Policy Targets	

And was able to see the packet traversing firewall (10.255.255.201 and 10.255.255.140 are its interfaces):



[root@ip-10-255-255-150 ec2-user]# ssh ec2-user@10.255.255.200
Permission denied (publickey).
[root@ip-10-255-255-150 ec2-user]#

And here is the tcpdump from the target host:
[root@ip-10-255-255-200 ec2-user]# tcpdump src 10.255.255.150
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

21:03:53.440273 IP 10.255.255.150.60118 > 10.255.255.200.ssh: Flags [S], seq 2098326363, win 26883, options [mss 1460,sackOK,TS val 843716 ecr 0,nop,wscale 7], length 0
...

With this Security group assigned to both hosts in my demo, the 10.255.255.150 and 10.255.255.200:

Where sg-e2264391 is the:

[ec2-user@ip-10-255-255-150 ~]$ date; ssh 10.255.255.200Fri Feb 16 13:29:42 UTC 2018Permission denied (publickey).[ec2-user@ip-10-255-255-150 ~]$ curl http://169.254.169.254/latest/meta-data/security-groupsTempSG1[ec2-user@ip-10-255-255-150 ~]$

[ec2-user@ip-10-255-255-200 ~]$ date; ssh 10.255.255.150

Fri Feb 16 13:30:04 UTC 2018

Permission denied (publickey).
[ec2-user@ip-10-255-255-200 ~]$ curl http://169.254.169.254/latest/meta-data/security-groups

TempSG1[ec2-user@ip-10-255-255-200 ~]$

And f you really want to be sure that the traffic in question was traversing the firewall and NOT a default VPC router:

and

[root@ip-10-255-255-200 ec2-user]# ifconfig | grep eth0
eth0 Link encap:Ethernet HWaddr 02:70:96:B0:44:80
[root@ip-10-255-255-200 ec2-user]#

[root@ip-10-255-255-200 ec2-user]# tcpdump -tttt -ne host 10.255.255.150
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
2018-02-15 16:01:28.245759 02:af:87:e2:04:c6 > 02:70:96:b0:44:80, ethertype IPv4 (0x0800), length 74: 10.255.255.150.39480 > 10.255.255.200.ssh: Flags [S], seq 3739857756, win 26883, options [mss 1460,sackOK,TS val 331468 ecr 0,nop,wscale 7], length 0

2018-02-15 16:01:28.245898 02:70:96:b0:44:80 > 02:af:87:e2:04:c6, ethertype IPv4 (0x0800), length 74: 10.255.255.200.ssh > 10.255.255.150.39480: Flags [S.], seq 3645387522, ack 3739857757, win 26847, options [mss 8961,sackOK,TS val 324911 ecr 331468,nop,wscale 7], length 0
2018-02-15 16:01:28.246290 02:af:87:e2:04:c6 > 02:70:96:b0:44:80, ethertype IPv4 (0x0800), length 66: 10.255.255.150.39480 > 10.255.255.200.ssh: Flags [.], ack 1, win 211, options [nop,nop,TS val 331469 ecr 324911], length 0
2018-02-15 16:01:28.246441 02:af:87:e2:04:c6 > 02:70:96:b0:44:80, ethertype IPv4 (0x0800), length 87: 10.255.255.150.39480 > 10.255.255.200.ssh: Flags [P.], seq 1:22, ack 1, win 211, options [nop,nop,TS val 331469 ecr 324911], length 21
2018-02-15 16:01:28.246450 02:70:96:b0:44:80 > 02:af:87:e2:04:c6, ethertype IPv4 (0x0800), length 66: 10.255.255.200.ssh > 10.255.255.150.39480: Flags [.], ack 22, win 210, options [nop,nop,TS val 324912 ecr 331469], length 0

The addition of the static routes could be either bootstrapped or included in AMIs, depending on your situation.

To verify that the instances residing in different subnets will remain isolated in the absence of the static routes, those were removed and we can see that the SSH connection attempt is timing out:

[ec2-user@ip-10-255-255-150 ~]$ route

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

default 10.255.255.129 0.0.0.0 UG 0 0 0 eth0

10.255.255.128 * 255.255.255.192 U 0 0 0 eth0

169.254.169.254 * 255.255.255.255 UH 0 0 0 eth0

[ec2-user@ip-10-255-255-150 ~]$ ssh ec2-user@10.255.255.200

ssh: connect to host 10.255.255.200 port 22: Connection timed out

[ec2-user@ip-10-255-255-150 ~]$

[ec2-user@ip-10-255-255-200 ~]$ route

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

default 10.255.255.193 0.0.0.0 UG 0 0 0 eth0

10.255.255.192 * 255.255.255.192 U 0 0 0 eth0

169.254.169.254 * 255.255.255.255 UH 0 0 0 eth0

[ec2-user@ip-10-255-255-200 ~]$ ssh ec2-user@10.255.255.150

ssh: connect to host 10.255.255.150 port 22: Connection timed out

[ec2-user@ip-10-255-255-200 ~]$

And reinstatement of the static routes results in:

[root@ip-10-255-255-150 ec2-user]# nano /etc/sysconfig/network-scripts/route-eth0

[root@ip-10-255-255-150 ec2-user]# reboot

[root@ip-10-255-255-150 ec2-user]#

Broadcast message from ec2-user@ip-10-255-255-150

(/dev/pts/0) at 16:54 ...
The system is going down for reboot NOW!

Using username "ec2-user".

Authenticating with public key "imported-openssh-key"

Last login: Fri Feb 16 16:42:28 2018 from xx.xx.xxx.98
__| __|_)

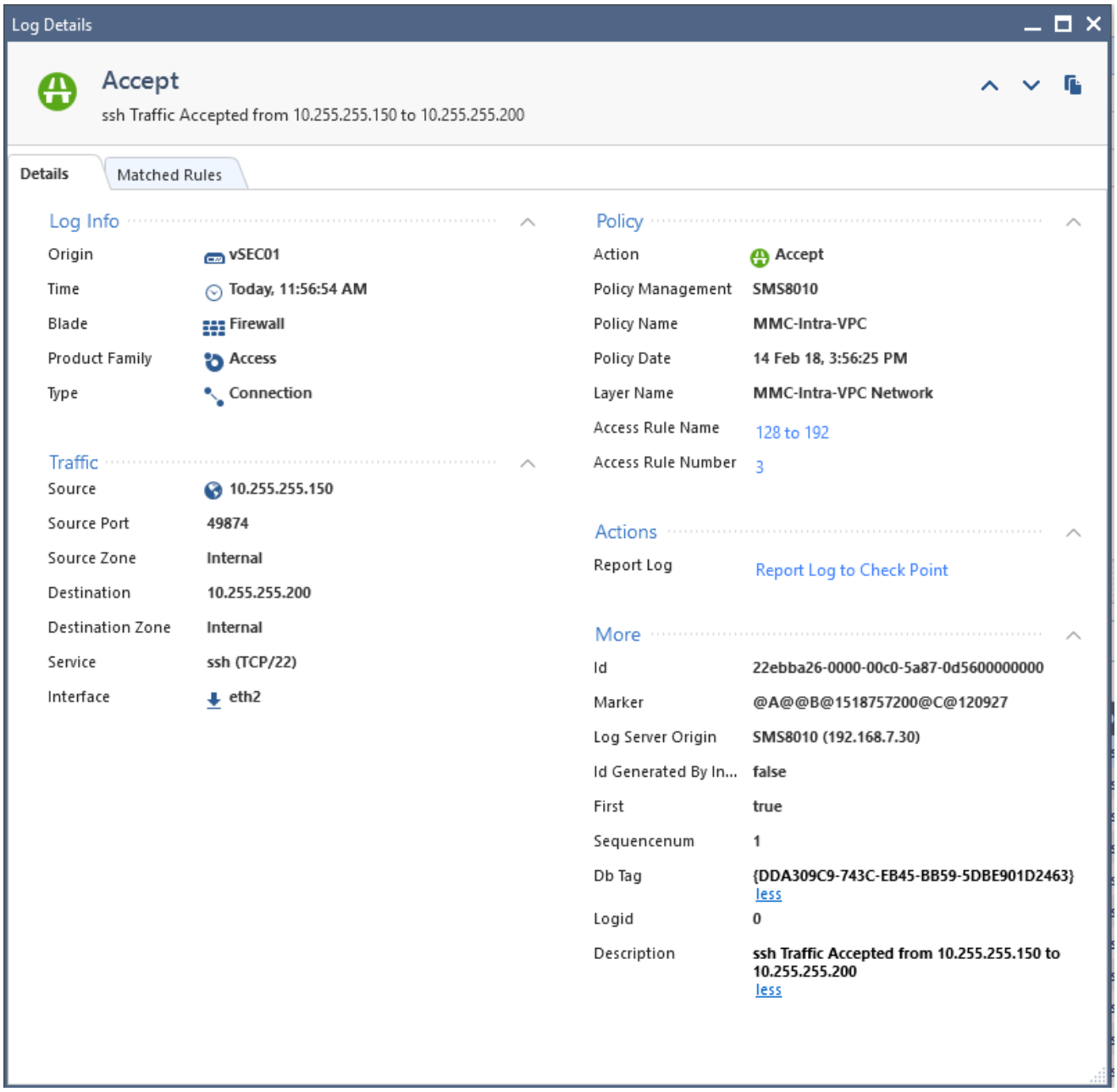
_| (/ Amazon Linux AMI

___|___|___|
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/

[ec2-user@ip-10-255-255-150 ~]$ ssh ec2-user@10.255.255.200

Permission denied (publickey).

[ec2-user@ip-10-255-255-150 ~]$



and:

root@ip-10-255-255-200 ec2-user]# nano /etc/sysconfig/network-scripts/route-eth0

[root@ip-10-255-255-200 ec2-user]# reboot

[root@ip-10-255-255-200 ec2-user]#

Broadcast message from ec2-user@ip-10-255-255-200

(/dev/pts/0) at 16:55 ...

The system is going down for reboot NOW!

Using username "ec2-user".

Authenticating with public key "imported-openssh-key"

Last login: Fri Feb 16 16:42:10 2018 from xx.xx.xxx.98

__| __|_)

_| (/ Amazon Linux AMI

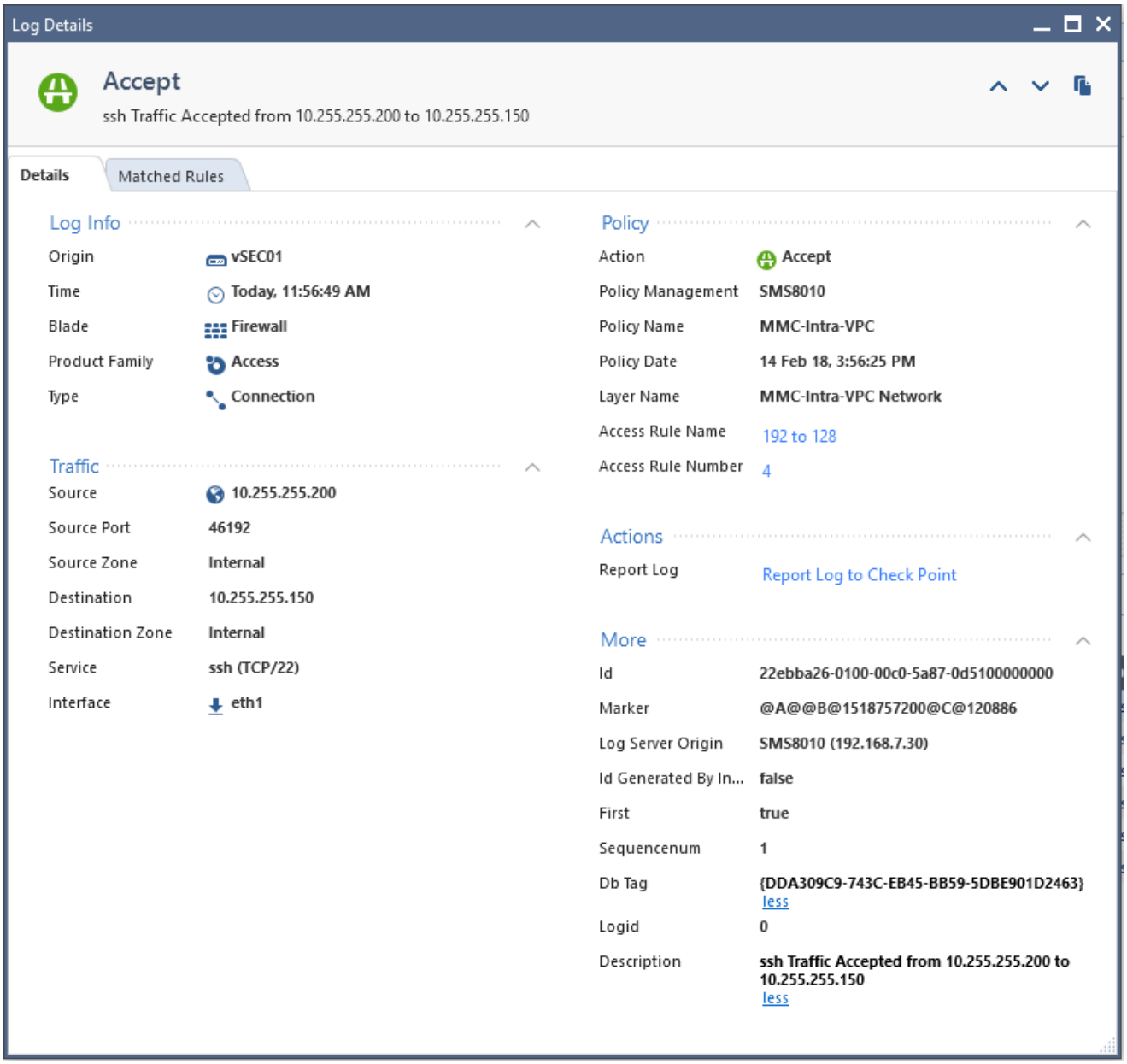
___|___|___|

https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/

[ec2-user@ip-10-255-255-200 ~]$ ssh ec2-user@10.255.255.150

Permission denied (publickey).

[ec2-user@ip-10-255-255-200 ~]$



This is the Gaia config for the vSEC used in this lab:

vSEC01> show configuration

#

Configuration of vSEC01

Language version: 13.1v1

#

Exported by admin on Thu Feb 15 13:47:33 2018

#

```
set installer policy check-for-updates-period 3
set installer policy periodically-self-update on
set installer policy send-cpuse-data off
set installer policy self-test install-policy off
set installer policy self-test network-link-up off
set installer policy self-test start-processes on
set arp table cache-size 4096
set arp table validity-timeout 60
set arp announce 2
set message banner on
set message motd on
set message caption off
set core-dump enable
set core-dump total 1000
set core-dump per_process 2
set clienv debug 0
set clienv echo-cmd off
set clienv output pretty
set clienv prompt "%M"
set clienv rows 24
set clienv syntax-check off
set dns primary 10.255.255.2
set dns secondary 8.8.8.8
set edition 64-bit
set expert-password-hash $blablabla
set format date dd-mmm-yyyy
set format time 24-hour
set format netmask Dotted
set hostname vSEC01
add allowed-client host any-host
set web table-refresh-rate 15
set web session-timeout 30
```

```
set web ssl-port 443
set web ssl3-enabled off
set web daemon-enable on
set inactivity-timeout 10
set ipv6-state off
add command api path /bin/api_wrap description "Start, stop, or check status of API server"
add command tecli path /bin/tecli_start description "Threat Emulation Blade shell"
set net-access telnet off
set ntp active on
set ntp server primary pool.ntp.org version 2
set user admin shell /bin/bash
set user admin password-hash $blablabla
set user monitor shell /etc/cli.sh
set user monitor password-hash *
set password-controls min-password-length 6
set password-controls complexity 2
set password-controls palindrome-check true
set password-controls history-checking true
set password-controls history-length 10
set password-controls password-expiration never
set password-controls expiration-warning-days 7
set password-controls expiration-lockout-days never
set password-controls force-change-when no
set password-controls deny-on-nonuse enable false
set password-controls deny-on-nonuse allowed-days 365
set password-controls deny-on-fail enable false
set password-controls deny-on-fail failures-allowed 10
set password-controls deny-on-fail allow-after 1200
set aaa tacacs-servers state off
set aaa radius-servers super-user-uid 96
set max-path-splits 8
set tracefile maxnum 10
```

```
set tracefile size 1
set syslog filename /var/log/messages
set syslog cplogs off
set syslog mgmtauditlogs on
set syslog auditlog permanent
set timezone America / New_York
set interface eth0 comments "vSEC01-Ext"
set interface eth0 link-speed 10G/full
set interface eth0 state on
set interface eth0 auto-negotiation on
set interface eth0 mtu 1500
set interface eth0 ipv4-address 10.255.255.22 mask-length 26
set interface eth1 comments "vSEC01-Int"
set interface eth1 link-speed 10G/full
set interface eth1 state on
set interface eth1 auto-negotiation on
set interface eth1 mtu 1500
set interface eth1 ipv4-address 10.255.255.201 mask-length 26
set interface eth2 comments "vSEC01-Proxy"
set interface eth2 link-speed 10G/full
set interface eth2 state on
set interface eth2 auto-negotiation on
set interface eth2 mtu 1500
set interface eth2 ipv4-address 10.255.255.140 mask-length 26
set interface lo state on
set interface lo ipv4-address 127.0.0.1 mask-length 8
add host name Simple01-LogicalServer-Web ipv4-address 10.255.255.23
set inbound-route-filter ospf2 accept-all-ipv4
set inbound-route-filter rip accept-all-ipv4
set management interface eth0
set ospf area backbone on
set rip update-interval default
```

set rip expire-interval default

set snmp mode default

set snmp agent off

set snmp agent-version v3-Only

set snmp traps trap authorizationError disable

set snmp traps trap biosFailure disable

set snmp traps trap coldStart disable

set snmp traps trap configurationChange disable

set snmp traps trap configurationSave disable

set snmp traps trap fanFailure disable

set snmp traps trap highVoltage disable

set snmp traps trap linkUpLinkDown disable

set snmp traps trap lowDiskSpace disable

set snmp traps trap lowVoltage disable

set snmp traps trap overTemperature disable

set snmp traps trap powerSupplyFailure disable

set snmp traps trap raidVolumeState disable

set snmp traps trap vrrpv2AuthFailure disable

set snmp traps trap vrrpv2NewMaster disable

set snmp traps trap vrrpv3NewMaster disable

set snmp traps trap vrrpv3ProtoError disable

set static-route default comment "To Subnet Router"

set static-route default nexthop gateway address 10.255.255.1 on

set static-route 10.100.100.0/24 comment "To Subnet Router for Peered VPC CIDR"

set static-route 10.100.100.0/24 nexthop gateway address 10.255.255.193 on

set static-route 10.255.255.128/26 comment "To Subnet Router"

set static-route 10.255.255.128/26 nexthop gateway address 10.255.255.129 on

set static-route 10.255.255.192/26 comment "To Subnet Router"

set static-route 10.255.255.192/26 nexthop gateway address 10.255.255.193 on

vSEC01>

Enjoy