Check Point®
SOFTWARE TECHNOLOGIES LTD.

CCSE

Content Awareness

Step by Step Configuration Guide

Intellectual Property

Table of Contents

1. Version Control

Version	Date	Notes	Created By	Release
1.0	18/12/2018	Student Workbook for LAB	Mazhar Minhas	Initial Release
1.1	31/04/2020	Formatting / Error Removal	Farooq Zafar	Final Release

2. Reference Document

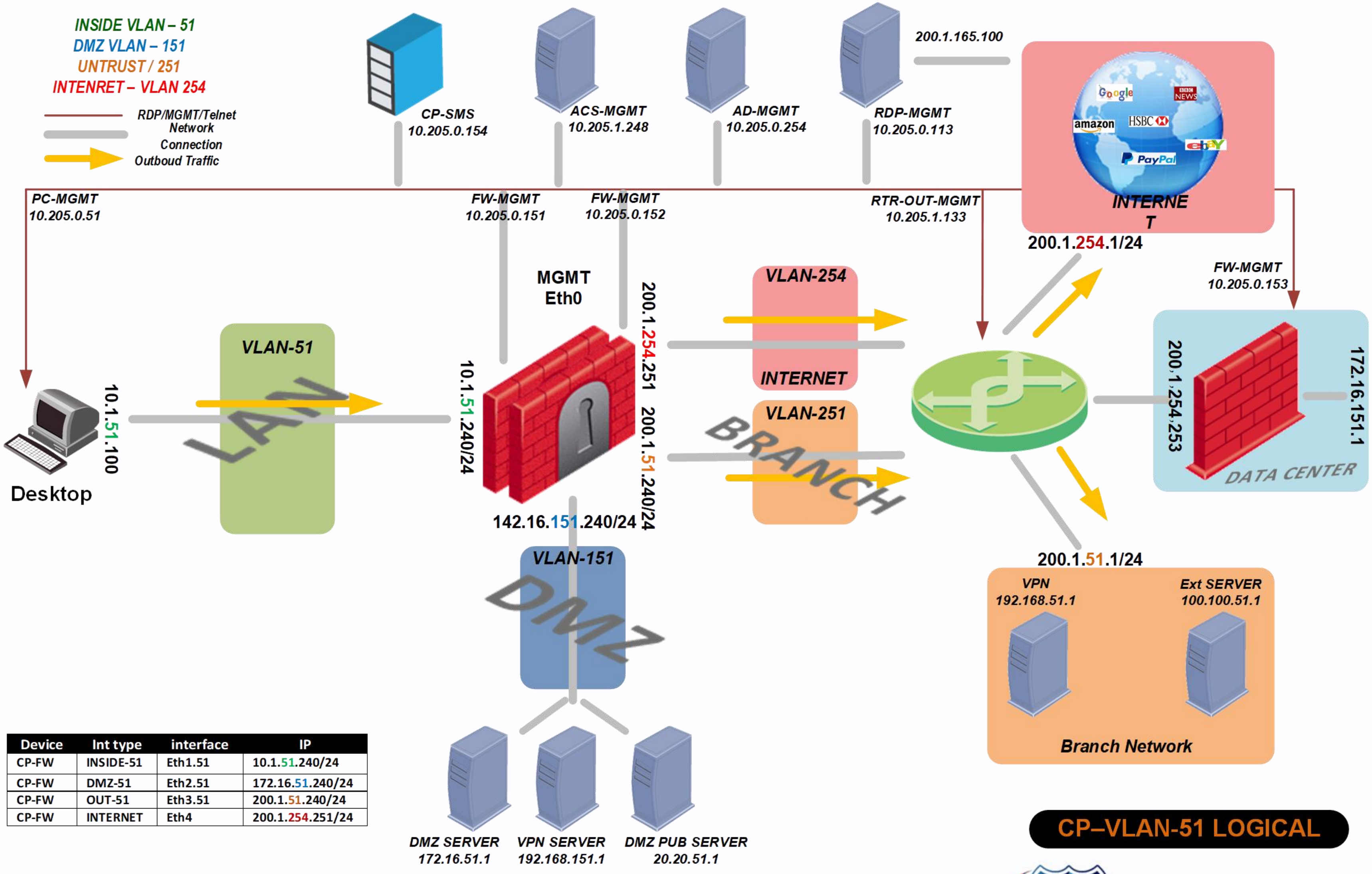
Click for the Reference document

3. Assumption

- ✓ We understand that delegate already understand L2/L3, Routing.
- ✓ The delegate already knows the "***Fortray Networks – Checkpoint Firewall"*** physical and logical connection.
- ✓ The delegate already has basis Troubleshooting skill, such as ping and trace.
- ✓ The delegate already has access to the "***Fortray Networks – Checkpoint Firewall"*** *Spreadsheet encompassing the Basic Layer, 2, 3 and allocated subnet information. For more details refer to the "**Student Folder".***
- ✓ This document is created to show an example for one topology only. The candidate needs to refer to his own topology and follow this step by step guide.
- ✓ We assume that delegate already have installed the VPN software and him/she have VPN user / Password. If any issue, contact our Technical team.
- ✓ Our VPN software is supported by PC, MAC, Android, and IOS devices.
- ✓ It's also assumed that delegate has access to PC/Laptop i5 with 4GB RAM.
- ✓ For optimal connectivity, we recommend at least 10MB Internet connection.
- ✓ We assume that we already have INTERNAL, DMZ, OUTISE interfaces are already configured.

4. Network Topology

The below network topology is just for information purpose only. Please refer to your student folder and your designated topology. If any doubt, please ask your instructor.



Device	Int type	interface	IP
CP-FW	INSIDE-51	Eth1.51	10.1.51.240/24
CP-FW	DMZ-51	Eth2.51	172.16.51.240/24
CP-FW	OUT-51	Eth3.51	200.1.51.240/24
CP-FW	INTERNET	Eth4	200.1.254.251/24

5. Check Point – Task: Content Awareness

According to new company policy no employee allowed to upload or download any windows executable file.

As a security engineer it is our job to block all executable files inside or outside of organization.

Summary of the steps

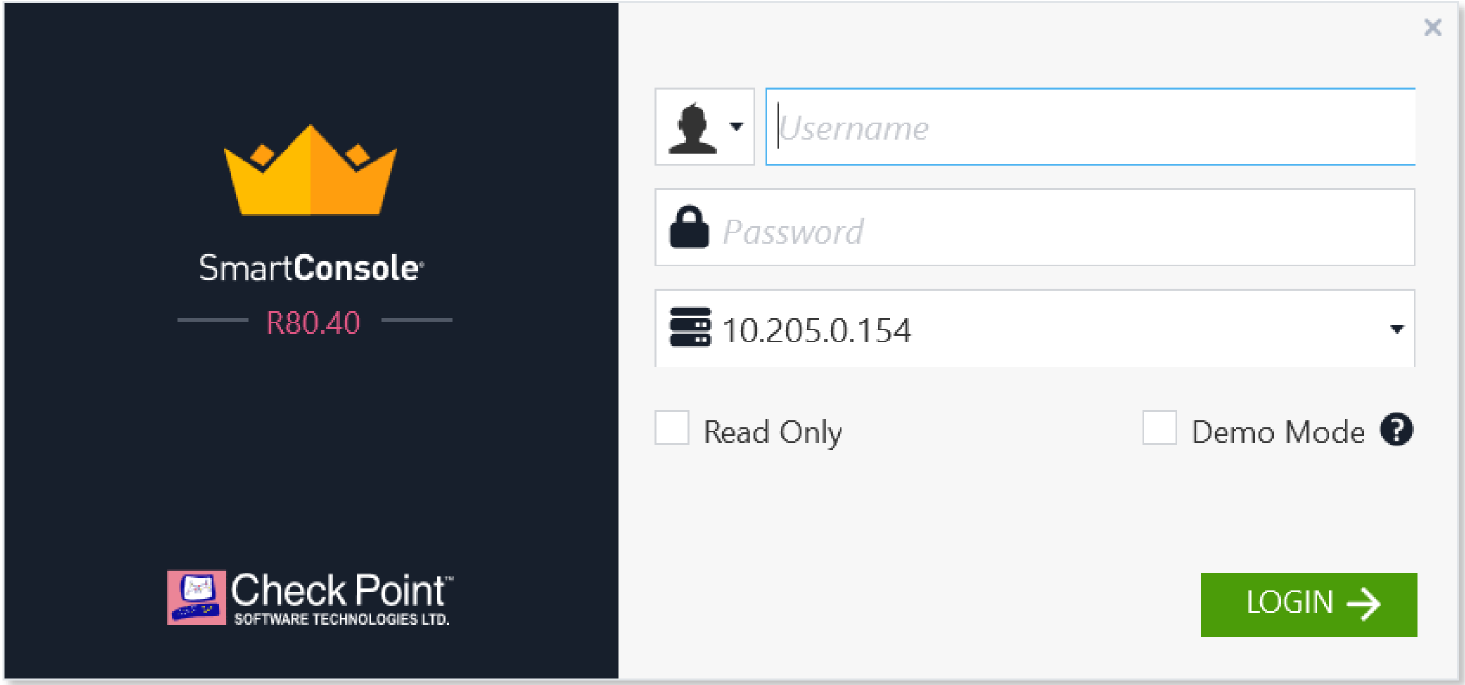
- Logging to Security Management Server
- Enabling Content Awareness on Desired Gateways
- Enabling Content Layer in Policy Editor
- Adding Rule to Block Executable files
- Verification

6. Check Point – Configuration: Content Awareness

In this section we will block executable files to be uploaded/downloaded.

6.1 Step 1: Login to SMS using SmartConsole

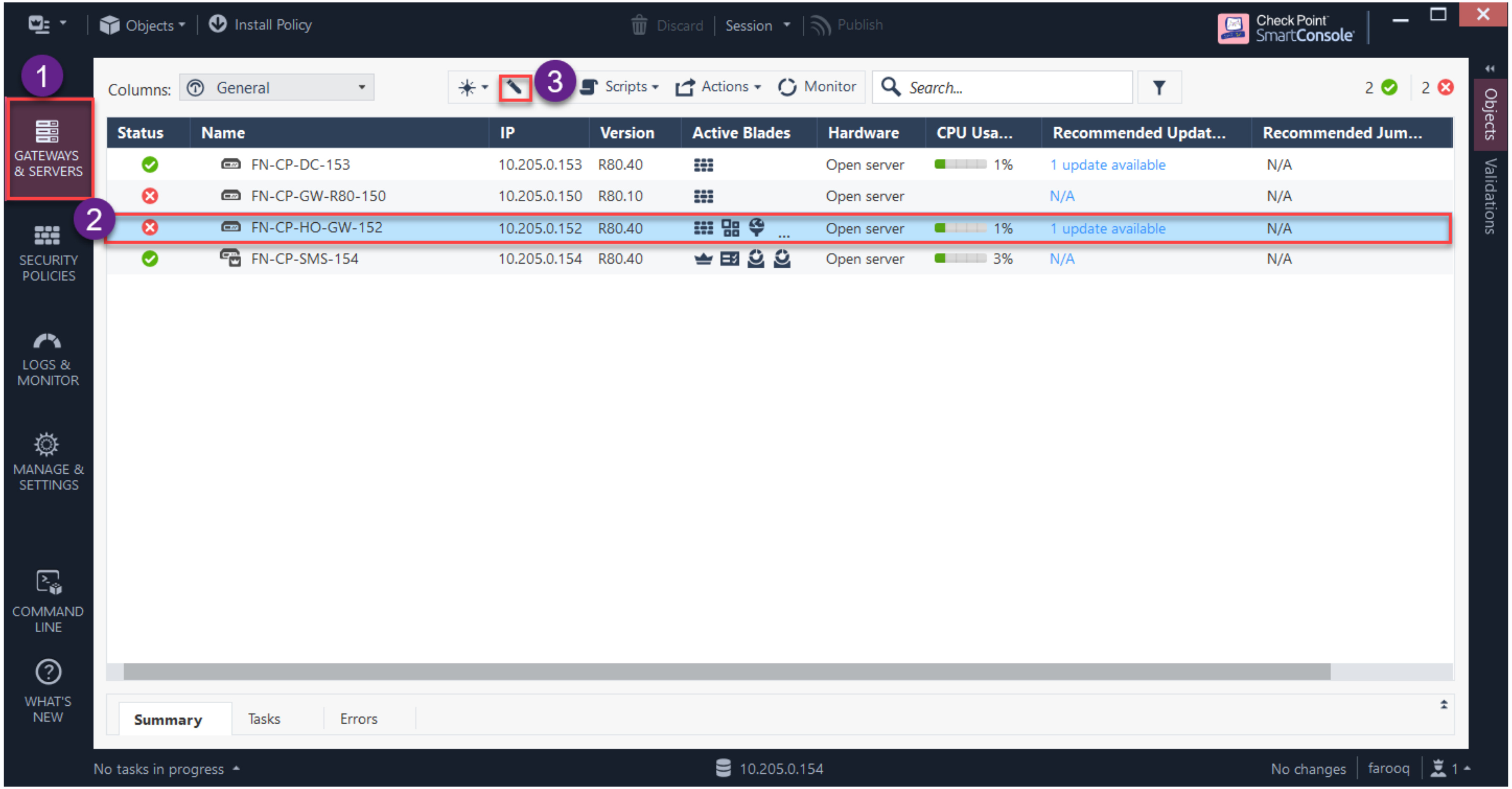
Open the SMS Application from your PC, login to SMS using default credential i.e., admin/admin123.



***Assumption:* This task assumes that we have already downloaded and installed the SMS R80.X software from the SMS via GUI.**

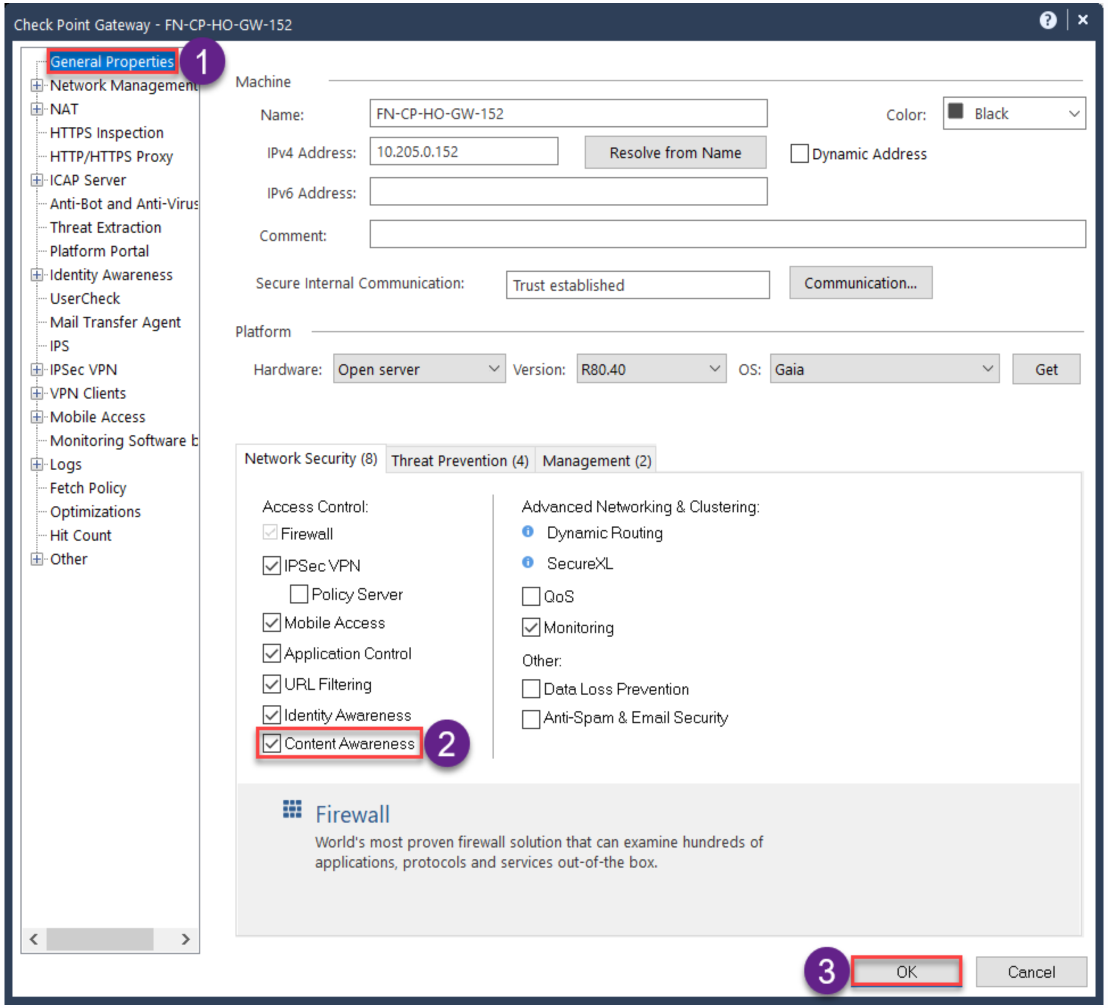
6.2 Step 2: Enabling Content Awareness Blade

Select GW from Gateways & Servers and click on Edit.



Status	Name	IP	Version	Active Blades	Hardware	CPU Usa...	Recommended Updat...	Recommended Jum...
✓	FN-CP-DC-153	10.205.0.153	R80.40		Open server	1%	1 update available	N/A
✗	FN-CP-GW-R80-150	10.205.0.150	R80.10		Open server		N/A	N/A
✗	FN-CP-HO-GW-152	10.205.0.152	R80.40	...	Open server	1%	1 update available	N/A
✓	FN-CP-SMS-154	10.205.0.154	R80.40		Open server	3%	N/A	N/A

Enable Content Awareness Blade by clicking on Checkbox in General Properties



Check Point Gateway - FN-CP-HO-GW-152

Machine

Name: FN-CP-HO-GW-152

Color: Black

IPv4 Address: 10.205.0.152

□ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: Open server

Version: R80.40

OS: Gaia

Access Control:

☑ Firewall

☑ IPSec VPN

□ Policy Server

☑ Mobile Access

☑ Application Control

☑ URL Filtering

☑ Identity Awareness

☑ Content Awareness

Advanced Networking & Clustering:

Dynamic Routing

SecureXL

□ QoS

☑ Monitoring

Other:

□ Data Loss Prevention

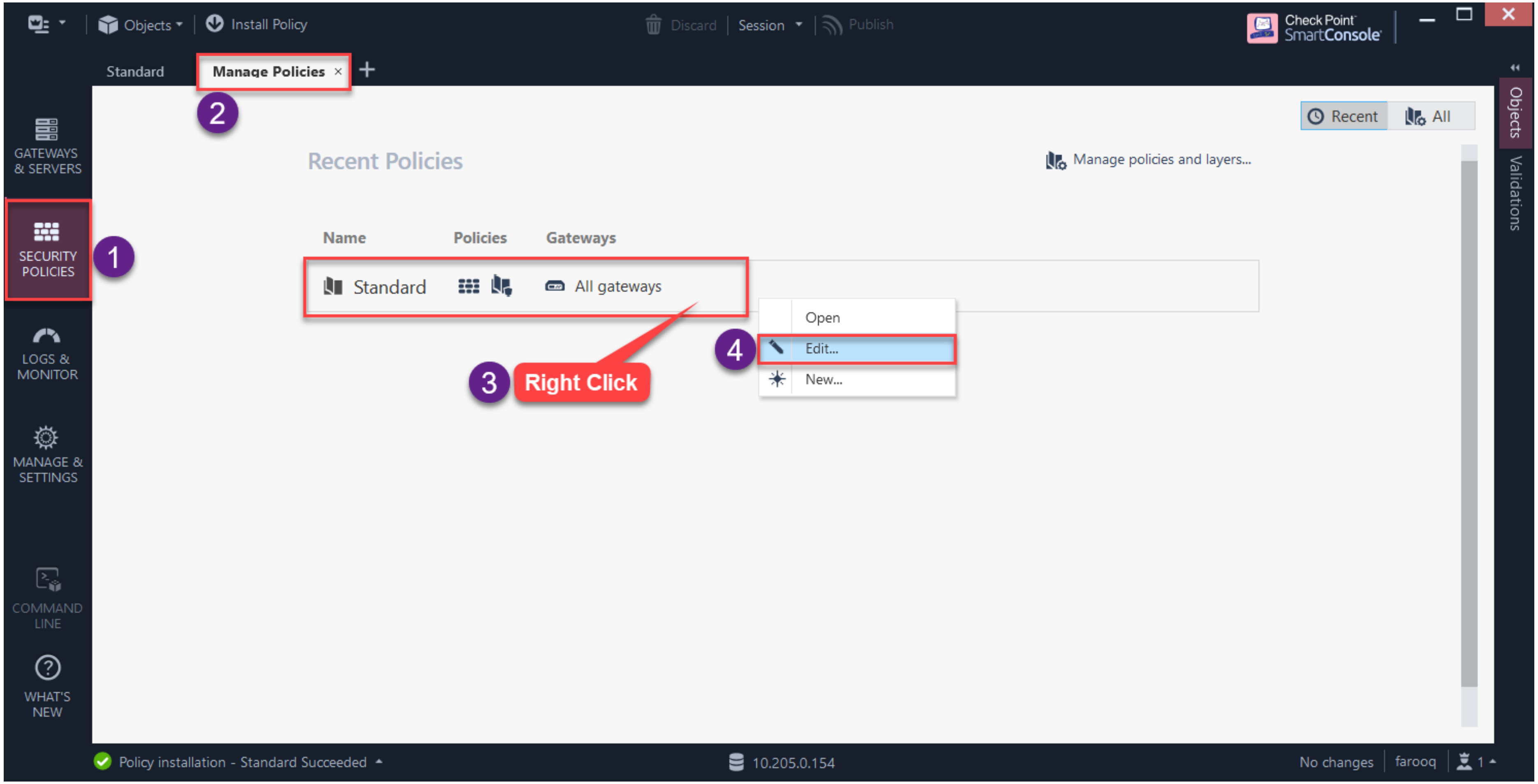
□ Anti-Spam & Email Security

Firewall

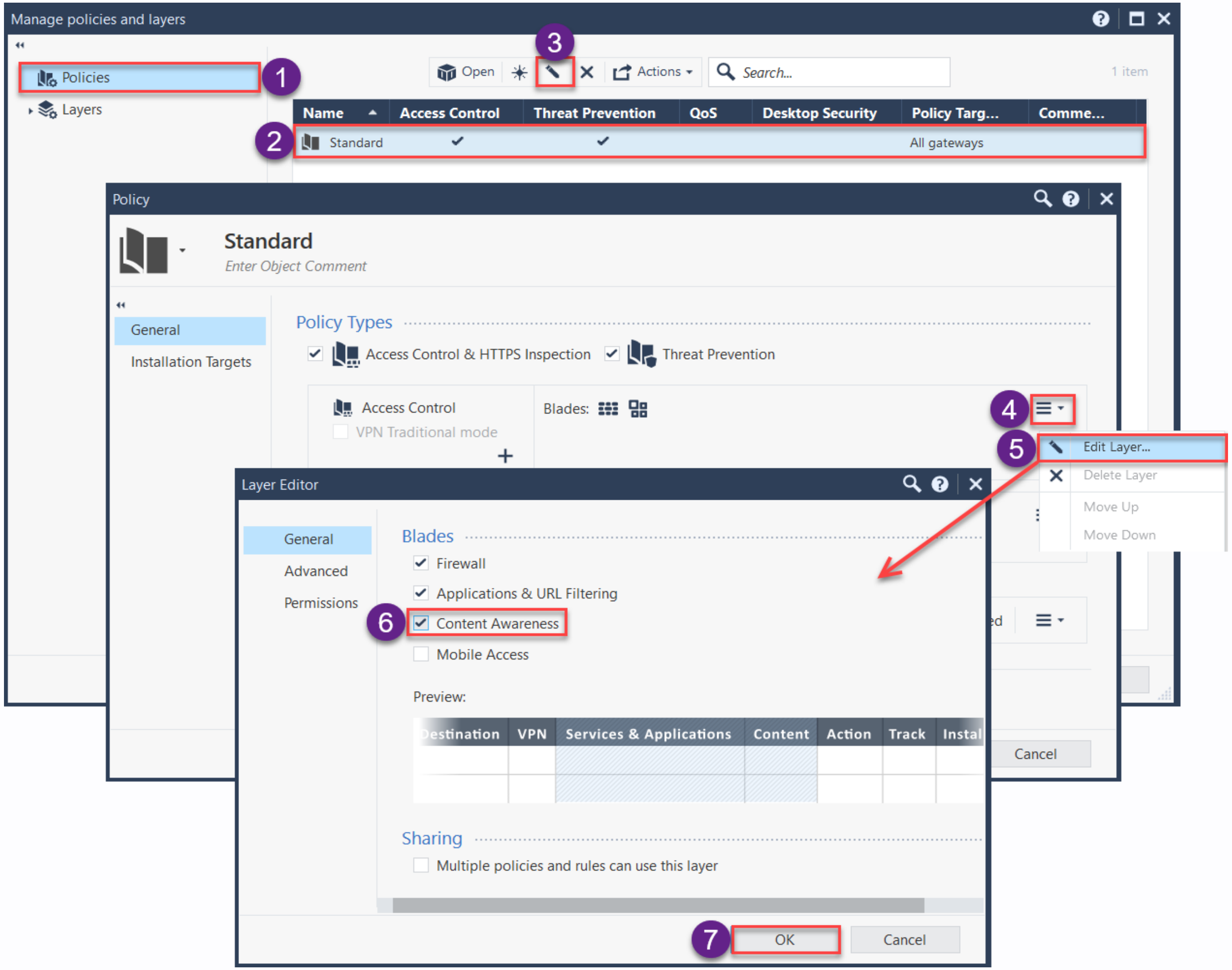
World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.

6.3 Step 3: Enabling Content Awareness Layer

Right Click on Standard Policy and Click on Edit in Security Policies > Manage Policies.

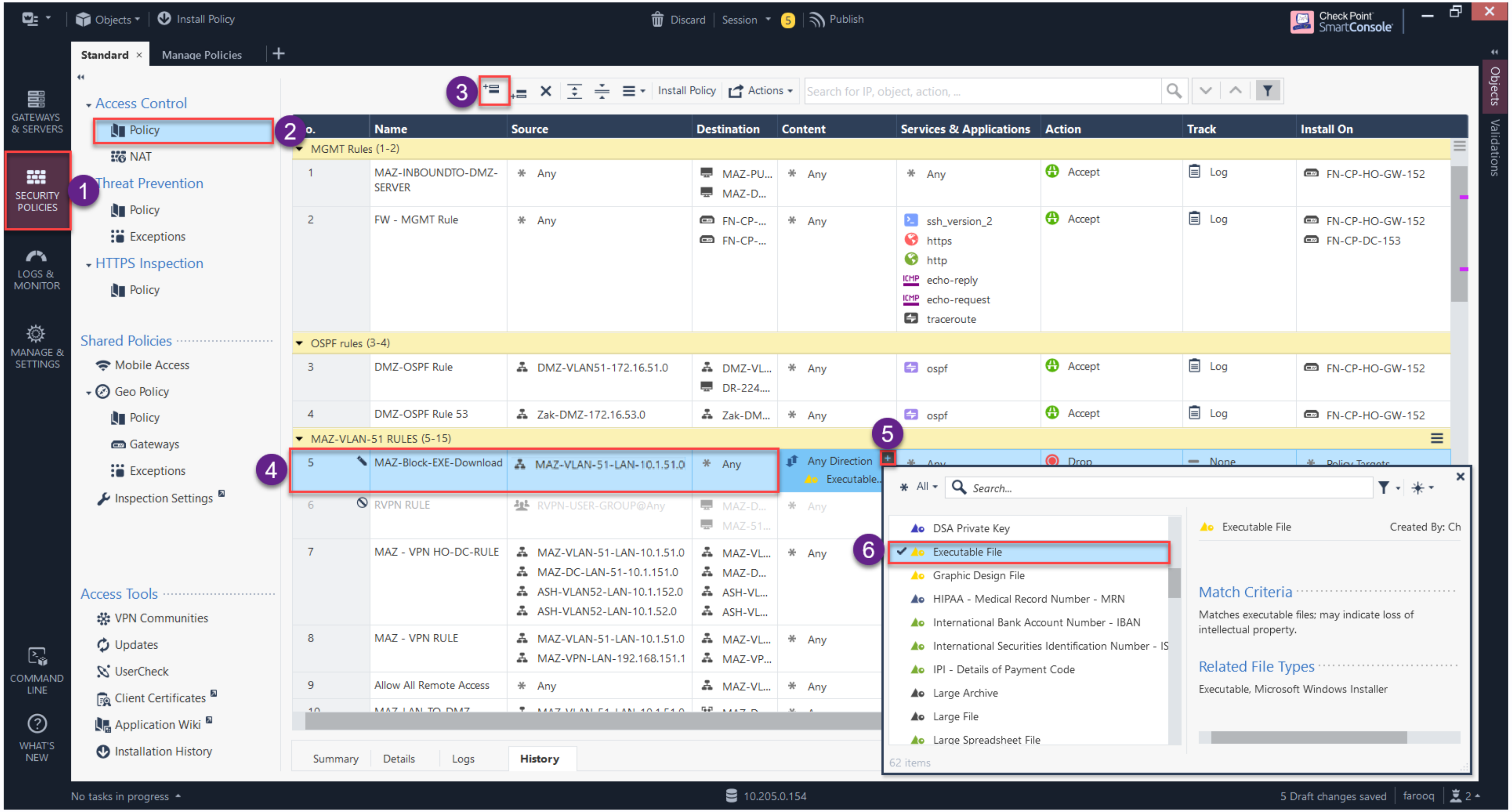


Then select Standard Policy in Policies and click Edit. In new setting window click on options > Edit Layer. Here Click on Content Awareness Checkbox and click OK. And click OK on all opened windows.



6.4 Step 4: Adding Policy to Block Executable Files

In Security Policies > Add Policy > Enter Values According to your VLAN. In content Field select Executable File in any Direction.



No.	Name	Source	Destination	Content	Services & Applications	Action	Track	Install On
MGMT Rules (1-2)								
1	MAZ-INBOUNDTO-DMZ-SERVER	Any	MAZ-PU... MAZ-D...	Any	Any	Accept	Log	FN-CP-HO-GW-152
2	FW - MGMT Rule	Any	FN-CP-... FN-CP-...	Any	ssh_version_2 https http echo-reply echo-request traceroute	Accept	Log	FN-CP-HO-GW-152 FN-CP-DC-153
OSPF rules (3-4)								
3	DMZ-OSPF Rule	DMZ-VLAN51-172.16.51.0	DMZ-VL... DR-224....	Any	ospf	Accept	Log	FN-CP-HO-GW-152
4	DMZ-OSPF Rule 53	Zak-DMZ-172.16.53.0	Zak-DM...	Any	ospf	Accept	Log	FN-CP-HO-GW-152
MAZ-VLAN-51 RULES (5-15)								
5	MAZ-Block-EXE-Download	MAZ-VLAN-51-LAN-10.1.51.0	Any	Any Direction Executable...	Any	Drop	None	Policy Targets
6	RVPN RULE	RVPN-USER-GROUP@Any	MAZ-D... MAZ-51...	Any				
7	MAZ - VPN HO-DC-RULE	MAZ-VLAN-51-LAN-10.1.51.0 MAZ-DC-LAN-51-10.1.151.0 ASH-VLAN52-LAN-10.1.152.0 ASH-VLAN52-LAN-10.1.52.0	MAZ-VL... MAZ-D... ASH-VL... ASH-VL...	Any				
8	MAZ - VPN RULE	MAZ-VLAN-51-LAN-10.1.51.0 MAZ-VPN-LAN-192.168.151.1	MAZ-VL... MAZ-VP...	Any				
9	Allow All Remote Access	Any	MAZ-VL...	Any				

All ▾ Search...

- DSA Private Key
- ✓ Executable File
- Graphic Design File
- HIPAA - Medical Record Number - MRN
- International Bank Account Number - IBAN
- International Securities Identification Number - IS
- IPI - Details of Payment Code
- Large Archive
- Large File
- Large Spreadsheet File

62 items

Executable File Created By: Ch

Match Criteria

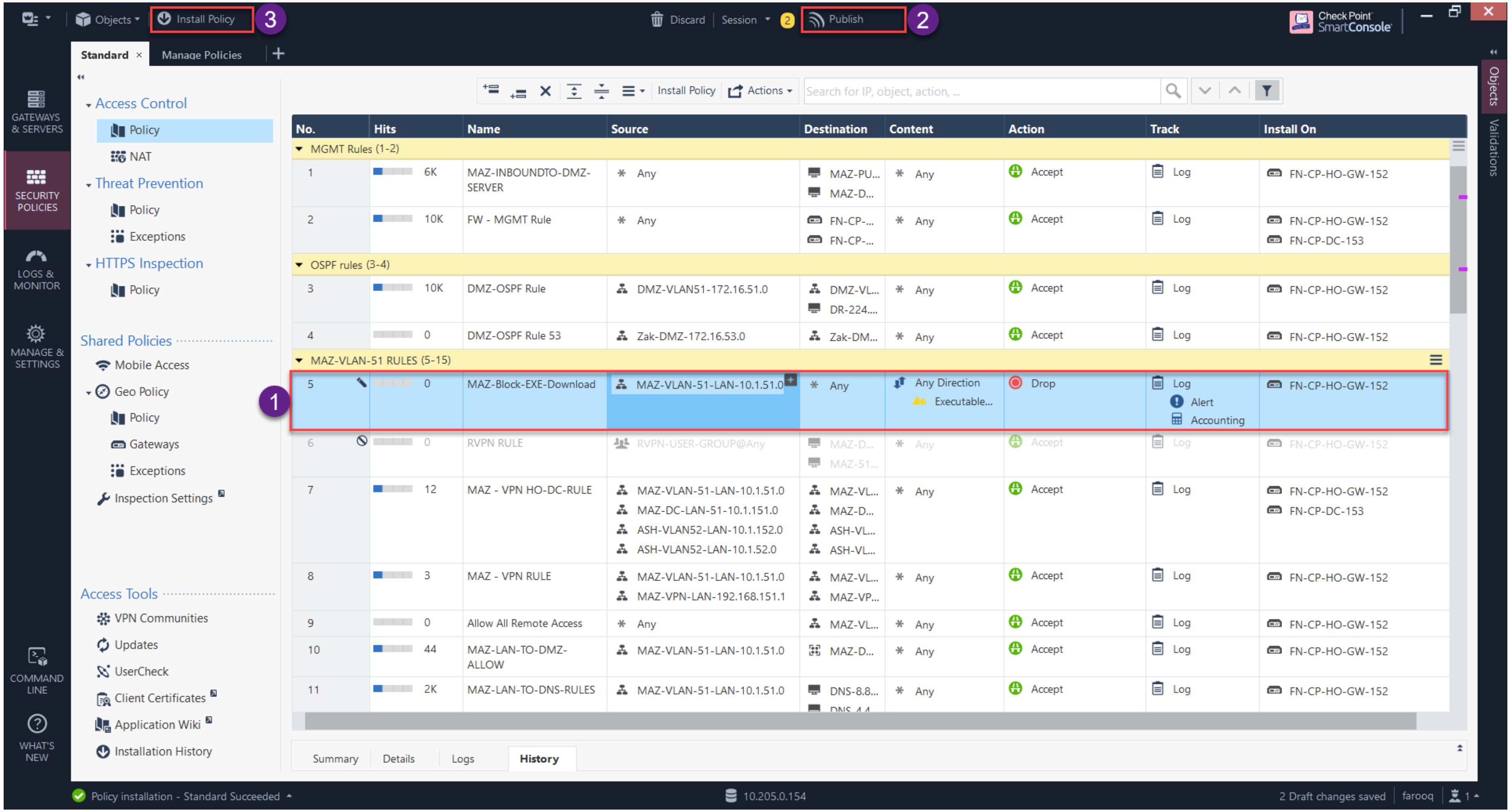
Matches executable files; may indicate loss of intellectual property.

Related File Types

Executable, Microsoft Windows Installer

No tasks in progress 10.205.0.154 5 Draft changes saved farooq 2

After completing Policy Fields click on Publish and then Install Policy.



No.	Hits	Name	Source	Destination	Content	Action	Track	Install On
MGMT Rules (1-2)								
1	6K	MAZ-INBOUNDTO-DMZ-SERVER	Any	MAZ-PU... MAZ-D...	Any	Accept	Log	FN-CP-HO-GW-152
2	10K	FW - MGMT Rule	Any	FN-CP-... FN-CP-...	Any	Accept	Log	FN-CP-HO-GW-152 FN-CP-DC-153
OSPF rules (3-4)								
3	10K	DMZ-OSPF Rule	DMZ-VLAN51-172.16.51.0	DMZ-VL... DR-224....	Any	Accept	Log	FN-CP-HO-GW-152
4	0	DMZ-OSPF Rule 53	Zak-DMZ-172.16.53.0	Zak-DM...	Any	Accept	Log	FN-CP-HO-GW-152
MAZ-VLAN-51 RULES (5-15)								
5	0	MAZ-Block-EXE-Download	MAZ-VLAN-51-LAN-10.1.51.0	Any	Any Direction Executable...	Drop	Log Alert Accounting	FN-CP-HO-GW-152
6	0	RVPN RULE	RVPN-USER-GROUP@Any	MAZ-D... MAZ-51...	Any	Accept	Log	FN-CP-HO-GW-152
7	12	MAZ - VPN HO-DC-RULE	MAZ-VLAN-51-LAN-10.1.51.0 MAZ-DC-LAN-51-10.1.151.0 ASH-VLAN52-LAN-10.1.152.0 ASH-VLAN52-LAN-10.1.52.0	MAZ-VL... MAZ-D... ASH-VL... ASH-VL...	Any	Accept	Log	FN-CP-HO-GW-152 FN-CP-DC-153
8	3	MAZ - VPN RULE	MAZ-VLAN-51-LAN-10.1.51.0 MAZ-VPN-LAN-192.168.151.1	MAZ-VL... MAZ-VP...	Any	Accept	Log	FN-CP-HO-GW-152
9	0	Allow All Remote Access	Any	MAZ-VL...	Any	Accept	Log	FN-CP-HO-GW-152
10	44	MAZ-LAN-TO-DMZ-ALLOW	MAZ-VLAN-51-LAN-10.1.51.0	MAZ-D...	Any	Accept	Log	FN-CP-HO-GW-152
11	2K	MAZ-LAN-TO-DNS-RULES	MAZ-VLAN-51-LAN-10.1.51.0	DNS-8.8... DNS 4.4	Any	Accept	Log	FN-CP-HO-GW-152

Policy installation - Standard Succeeded

10.205.0.154

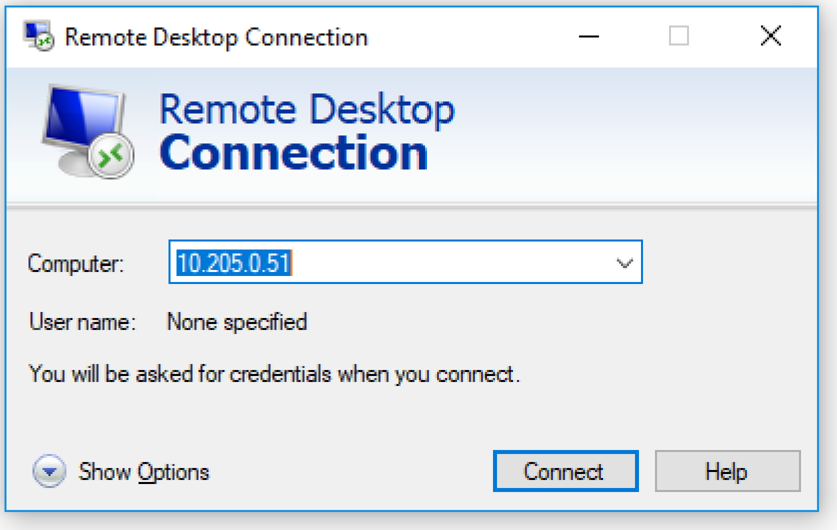
2 Draft changes saved | farooq | 1

7. Verification

To verify Content Awareness and created policy we need to do following steps

7.1 Step 1: Login to Remote Test PC

Login to your assigned Remote Test PC using **Remote Desktop Connection** Application, Use Administrator/Cisco as username/password to connect.

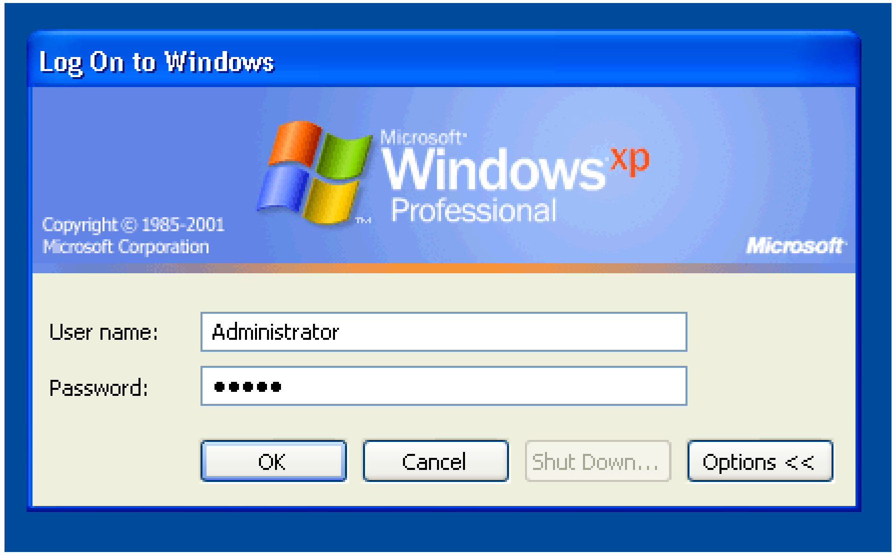


Remote Desktop Connection

Computer: 10.205.0.51

User name: None specified

You will be asked for credentials when you connect.



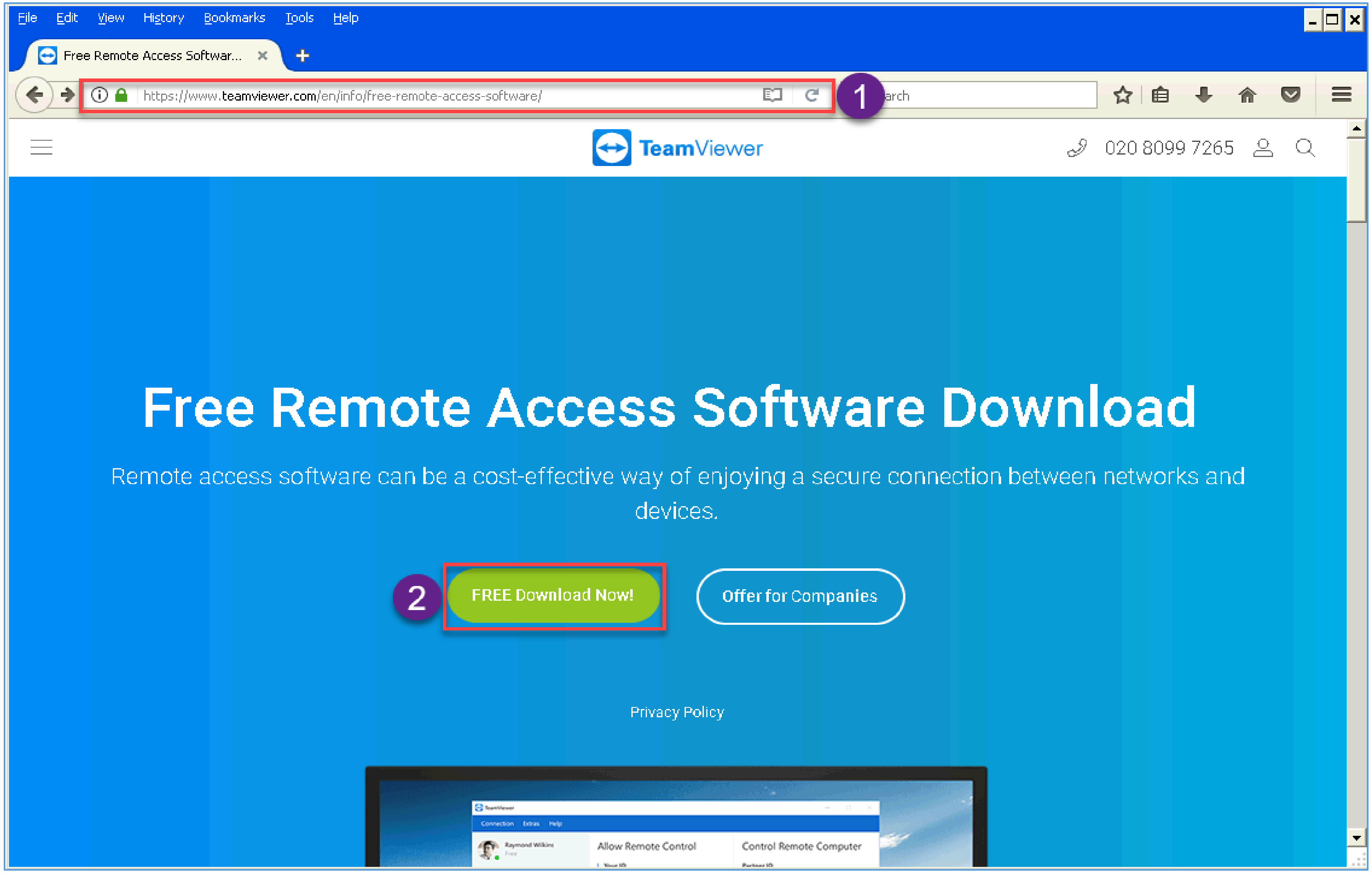
Log On to Windows

User name: Administrator

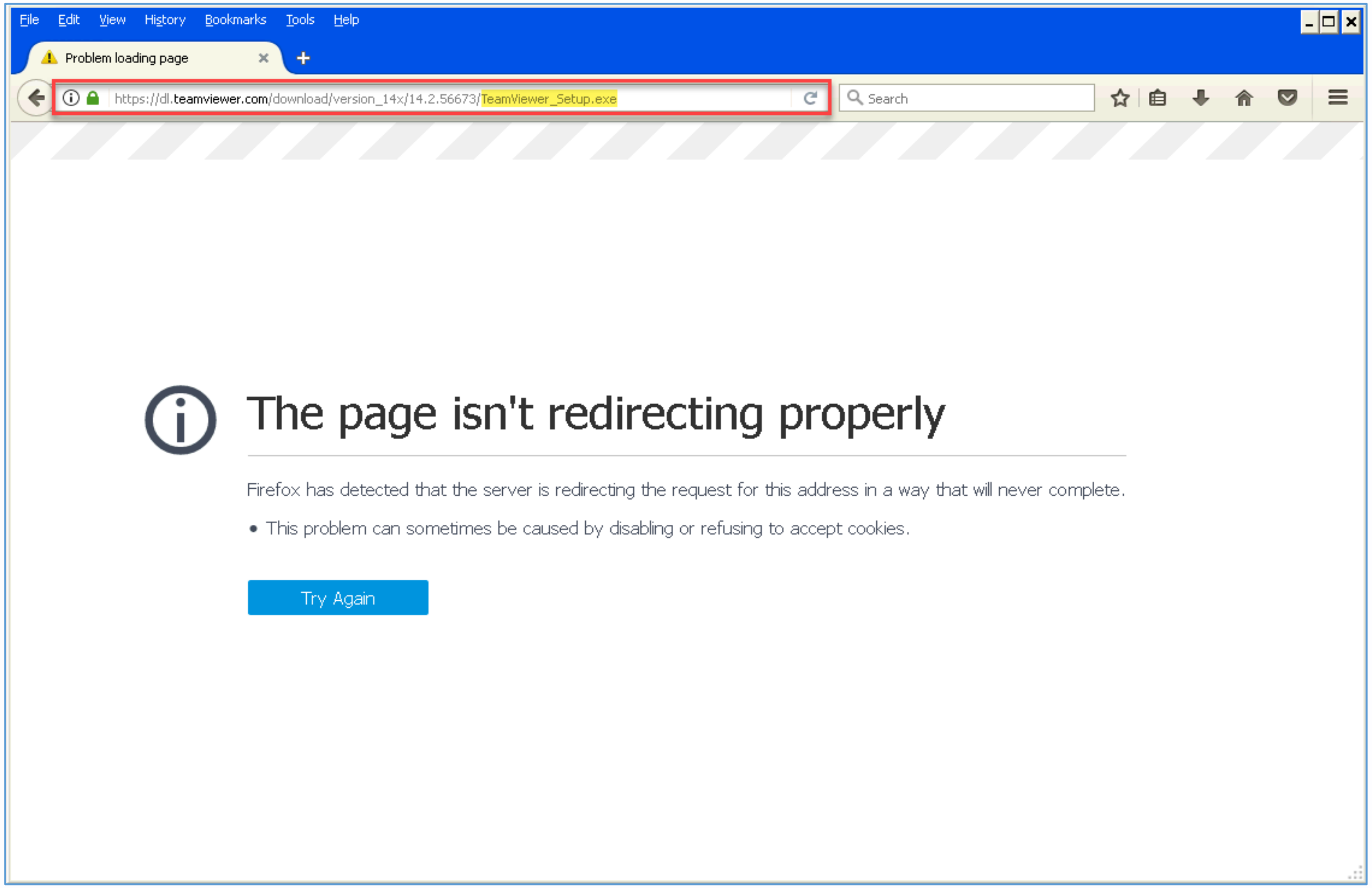
Password: ●●●●●

7.2 Step 2: Downloading Some Executable File

Open web browser and try to download and executable file. Here we are going to download TeamViewer.


File Edit View History Bookmarks Tools Help
Free Remote Access Softwar...
https://www.teamviewer.com/en/info/free-remote-access-software/
1
arch
TeamViewer
020 8099 7265
Free Remote Access Software Download
Remote access software can be a cost-effective way of enjoying a secure connection between networks and devices.
2
FREE Download Now!
Offer for Companies
Privacy Policy
Allow Remote Control
Control Remote Computer

We tried to download executable file and failed.



File Edit View History Bookmarks Tools Help
Problem loading page
https://dl.teamviewer.com/download/version_14x/14.2.56673/TeamViewer_Setup.exe
Search

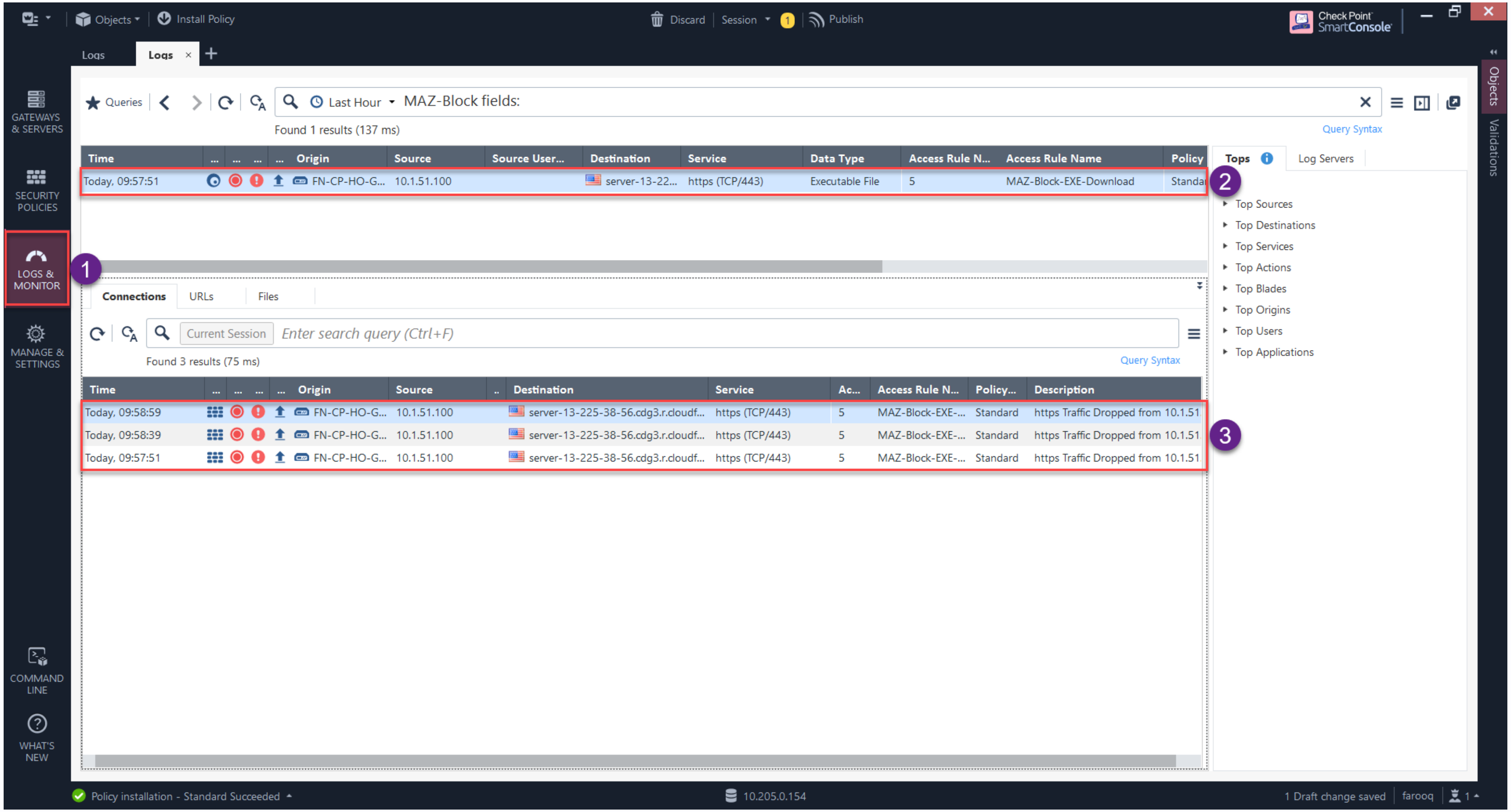
The page isn't redirecting properly

Firefox has detected that the server is redirecting the request for this address in a way that will never complete.

- This problem can sometimes be caused by disabling or refusing to accept cookies.

7.3 Step 3: Verification Via Logs

In SMS click on LOGS & MONITOR, here we can see logs.



MAZ-Block fields:

Found 1 results (137 ms)

Time	...	...	...	...	Origin	Source	Source User...	Destination	Service	Data Type	Access Rule N...	Access Rule Name	Policy
Today, 09:57:51					FN-CP-HO-G...	10.1.51.100		server-13-22...	https (TCP/443)	Executable File	5	MAZ-Block-EXE-Download	Standa

Found 3 results (75 ms)

Time	...	...	...	...	Origin	Source	..	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 09:58:59					FN-CP-HO-G...	10.1.51.100		server-13-225-38-56.cdg3.r.cloudf...	https (TCP/443)	5	MAZ-Block-EXE-...	Standard	https Traffic Dropped from 10.1.51
Today, 09:58:39					FN-CP-HO-G...	10.1.51.100		server-13-225-38-56.cdg3.r.cloudf...	https (TCP/443)	5	MAZ-Block-EXE-...	Standard	https Traffic Dropped from 10.1.51
Today, 09:57:51					FN-CP-HO-G...	10.1.51.100		server-13-225-38-56.cdg3.r.cloudf...	https (TCP/443)	5	MAZ-Block-EXE-...	Standard	https Traffic Dropped from 10.1.51

Thanks, and Good Luck