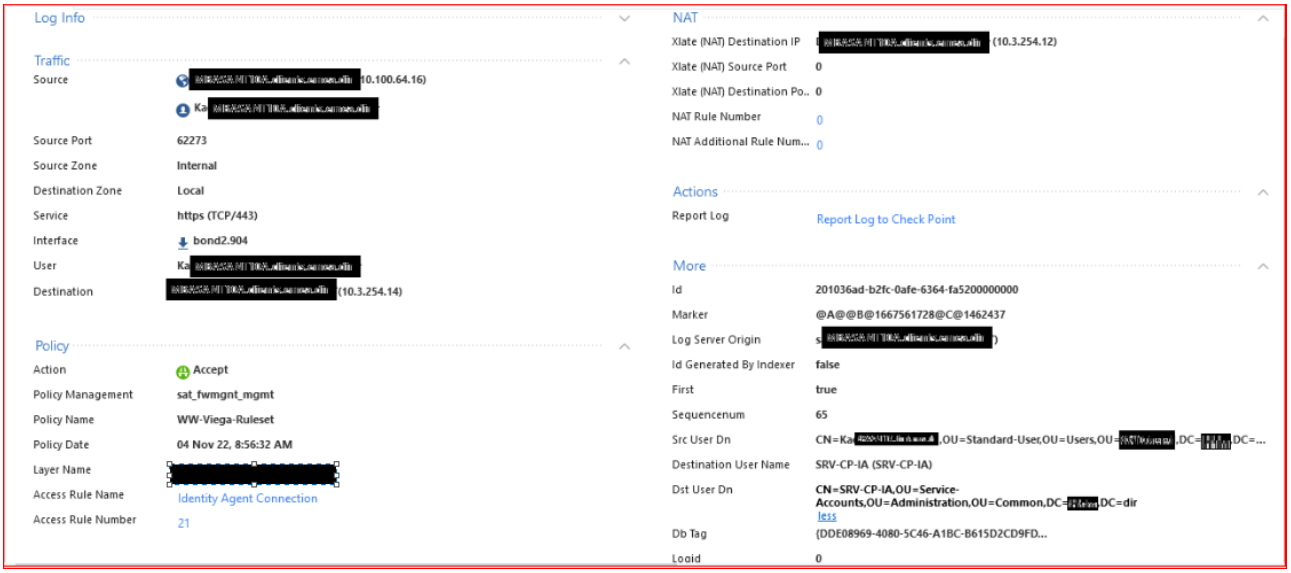
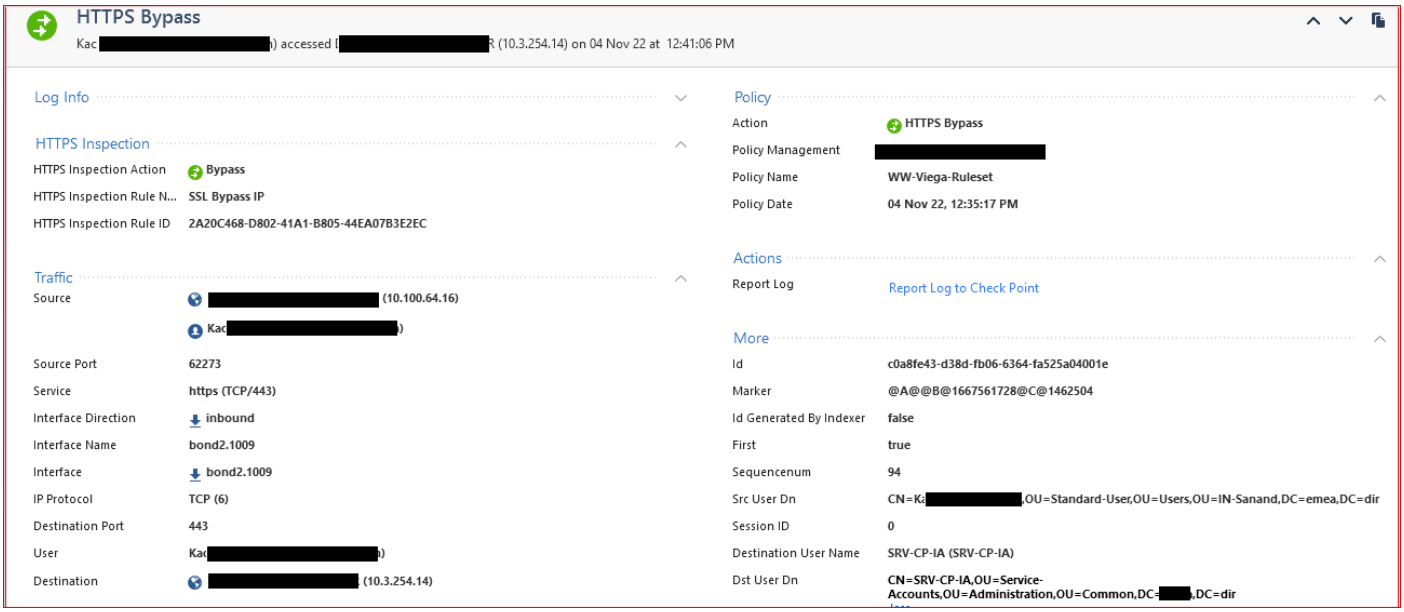
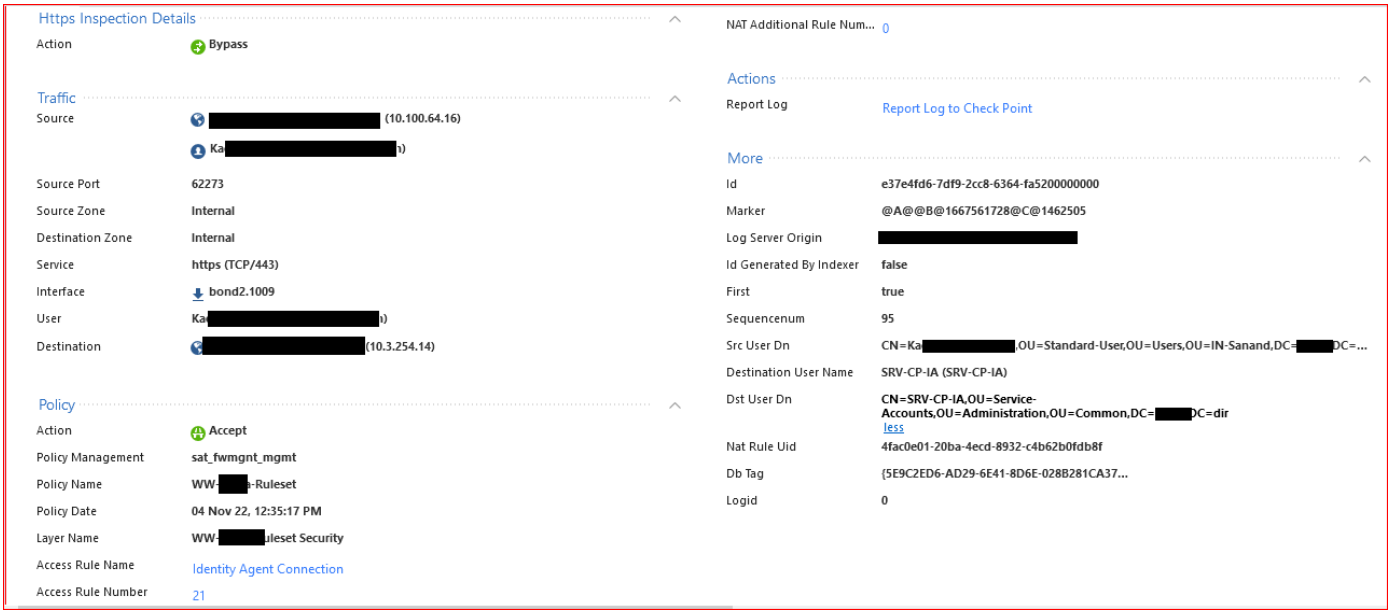
1.


Log Info
Traffic
Source
(10.100.64.16)
Source Port
62273
Source Zone
Internal
Destination Zone
Local
Service
https (TCP/443)
Interface
bond2.904
User
Destination
(10.3.254.14)
Policy
Action
Accept
Policy Management
sat_fwmgnt_mgmt
Policy Name
WW-Viega-Ruleset
Policy Date
04 Nov 22, 8:56:32 AM
Layer Name
Access Rule Name
Identity Agent Connection
Access Rule Number
21
NAT
Xlate (NAT) Destination IP
(10.3.254.12)
Xlate (NAT) Source Port
0
Xlate (NAT) Destination Po..
0
NAT Rule Number
0
NAT Additional Rule Num...
0
Actions
Report Log
Report Log to Check Point
More
Id
201036ad-b2fc-0afe-6364-fa5200000000
Marker
@A@@B@1667561728@C@1462437
Log Server Origin
Id Generated By Indexer
false
First
true
Sequencenum
65
Src User Dn
CN=Ka
,OU=Standard-User,OU=Users,OU=
,DC=
,DC=...
Destination User Name
SRV-CP-IA (SRV-CP-IA)
Dst User Dn
CN=SRV-CP-IA,OU=Service-Accounts,OU=Administration,OU=Common,DC=
,DC=dir
less
Db Tag
{DDE08969-4080-5C46-A1BC-B615D2CD9FD...
Logid
0

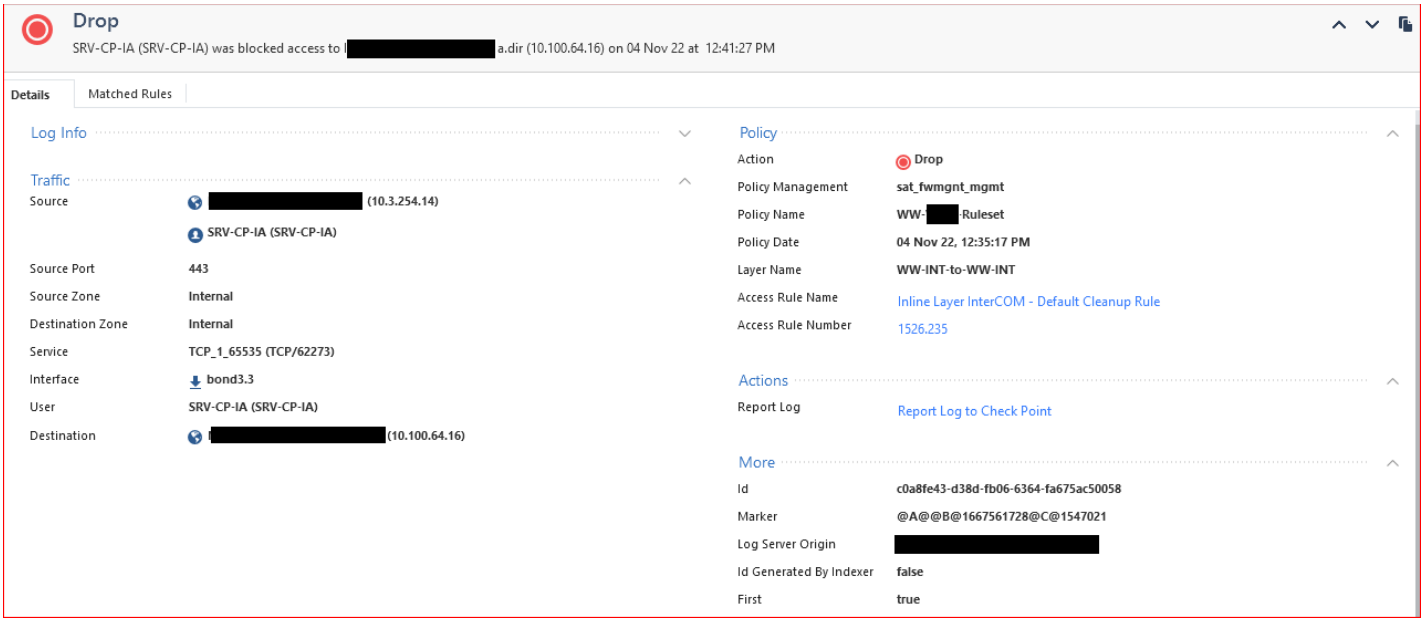
2.


HTTPS Bypass
Kac
) accessed
R (10.3.254.14) on 04 Nov 22 at 12:41:06 PM
Log Info
HTTPS Inspection
HTTPS Inspection Action
Bypass
HTTPS Inspection Rule N...
SSL Bypass IP
HTTPS Inspection Rule ID
2A20C468-D802-41A1-B805-44EA07B3E2EC
Traffic
Source
(10.100.64.16)
Kac
)
Source Port
62273
Service
https (TCP/443)
Interface Direction
inbound
Interface Name
bond2.1009
Interface
bond2.1009
IP Protocol
TCP (6)
Destination Port
443
User
Kac
)
Destination
(10.3.254.14)
Policy
Action
HTTPS Bypass
Policy Management
Policy Name
WW-Viega-Ruleset
Policy Date
04 Nov 22, 12:35:17 PM
Actions
Report Log
Report Log to Check Point
More
Id
c0a8fe43-d38d-fb06-6364-fa525a04001e
Marker
@A@@B@1667561728@C@1462504
Id Generated By Indexer
false
First
true
Sequencenum
94
Src User Dn
CN=K
,OU=Standard-User,OU=Users,OU=IN-Sanand,DC=emea,DC=dir
Session ID
0
Destination User Name
SRV-CP-IA (SRV-CP-IA)
Dst User Dn
CN=SRV-CP-IA,OU=Service-Accounts,OU=Administration,OU=Common,DC=
.DC=dir

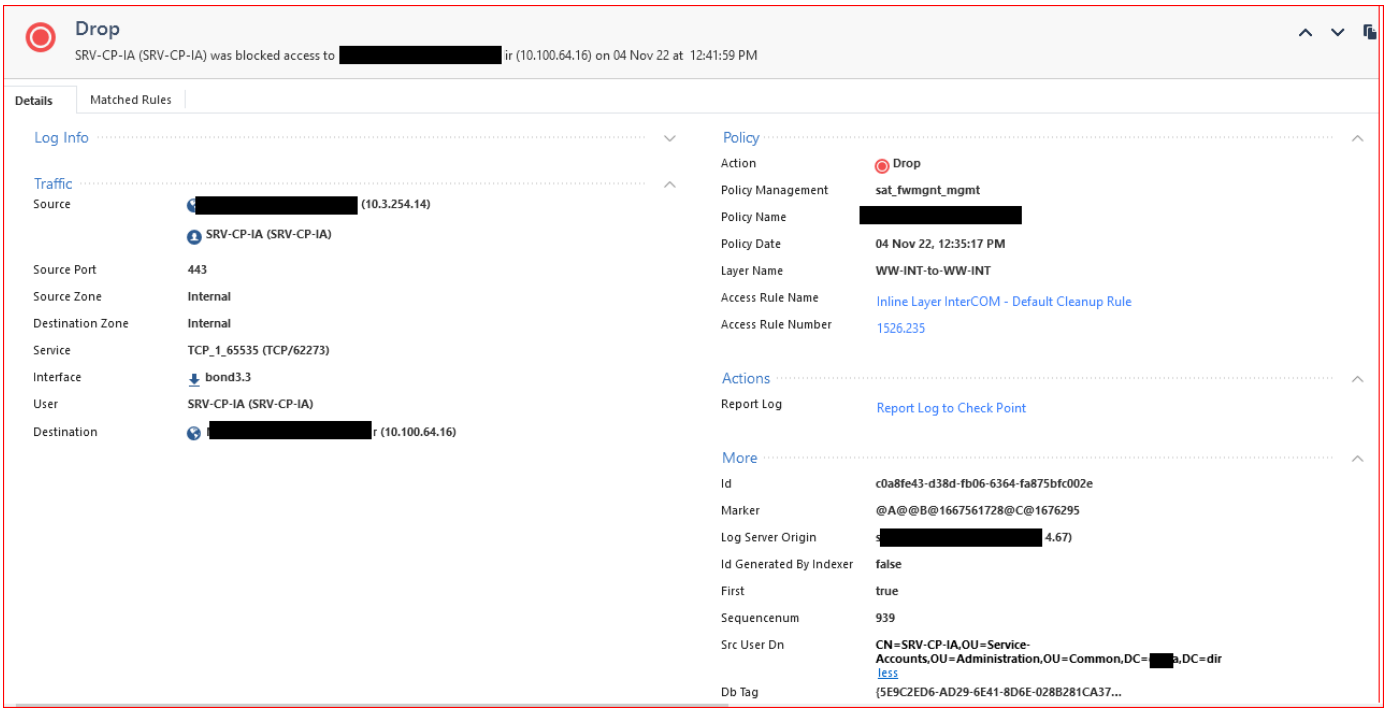
3.


Https Inspection Details
Action
Bypass
Traffic
Source
(10.100.64.16)
Source Port
62273
Source Zone
Internal
Destination Zone
Internal
Service
https (TCP/443)
Interface
bond2.1009
User
Destination
(10.3.254.14)
Policy
Action
Accept
Policy Management
sat_fwmgnt_mgmt
Policy Name
Policy Date
04 Nov 22, 12:35:17 PM
Layer Name
Access Rule Name
Identity Agent Connection
Access Rule Number
21
NAT Additional Rule Num...
0
Actions
Report Log
Report Log to Check Point
More
Id
e37e4fd6-7df9-2cc8-6364-fa5200000000
Marker
@A@@B@1667561728@C@1462505
Log Server Origin
Id Generated By Indexer
false
First
true
Sequencenum
95
Src User Dn
Destination User Name
SRV-CP-IA (SRV-CP-IA)
Dst User Dn
CN=SRV-CP-IA,OU=Service-Accounts,OU=Administration,OU=Common,DC=
DC=dir
less
Nat Rule Uid
4fac0e01-20ba-4ecd-8932-c4b62b0fdb8f
Db Tag
{5E9C2ED6-AD29-6E41-8D6E-028B281CA37...
Logid
0

4.


Drop
SRV-CP-IA (SRV-CP-IA) was blocked access to
a.dir (10.100.64.16) on 04 Nov 22 at 12:41:27 PM
Details
Matched Rules
Log Info
Traffic
Source
(10.3.254.14)
SRV-CP-IA (SRV-CP-IA)
Source Port
443
Source Zone
Internal
Destination Zone
Internal
Service
TCP_1_65535 (TCP/62273)
Interface
bond3.3
User
SRV-CP-IA (SRV-CP-IA)
Destination
(10.100.64.16)
Policy
Action
Drop
Policy Management
sat_fwmgnt_mgmt
Policy Name
Ruleset
Policy Date
04 Nov 22, 12:35:17 PM
Layer Name
WW-INT-to-WW-INT
Access Rule Name
Inline Layer InterCOM - Default Cleanup Rule
Access Rule Number
1526.235
Actions
Report Log
Report Log to Check Point
More
Id
c0a8fe43-d38d-fb06-6364-fa675ac50058
Marker
@A@@B@1667561728@C@1547021
Log Server Origin
Id Generated By Indexer
false
First
true

5.


Drop
SRV-CP-IA (SRV-CP-IA) was blocked access to [redacted] ir (10.100.64.16) on 04 Nov 22 at 12:41:59 PM
Details
Matched Rules
Log Info
Traffic
Source
[redacted] (10.3.254.14)
SRV-CP-IA (SRV-CP-IA)
Source Port
443
Source Zone
Internal
Destination Zone
Internal
Service
TCP_1_65535 (TCP/62273)
Interface
bond3.3
User
SRV-CP-IA (SRV-CP-IA)
Destination
[redacted] r (10.100.64.16)
Policy
Action
Drop
Policy Management
sat_fwmgnt_mgmt
Policy Name
[redacted]
Policy Date
04 Nov 22, 12:35:17 PM
Layer Name
WW-INT-to-WW-INT
Access Rule Name
Inline Layer InterCOM - Default Cleanup Rule
Access Rule Number
1526.235
Actions
Report Log
Report Log to Check Point
More
Id
c0a8fe43-d38d-fb06-6364-fa875bfc002e
Marker
@A@@B@1667561728@C@1676295
Log Server Origin
s[redacted] 4.67)
Id Generated By Indexer
false
First
true
Sequencenum
939
Src User Dn
CN=SRV-CP-IA,OU=Service-Accounts,OU=Administration,OU=Common,DC=[redacted]a,DC=dir
less
Db Tag
{5E9C2ED6-AD29-6E41-8D6E-028B281CA37...