**Firestorm: CASB Support for Applications and Activities**

**Introduction**

==========

CASB is to provide inline activity control on a limited set of cloud applications.

Cloud applications supported :

* Meta (Facebook) Messenger
* Office365\_Word
* Office365\_Excel
* Office365\_Powerpoint

**2  Functionality**

============

CASB is a new L7 service which provides inline application activity control. CASB helps organizations to protect and control access to cloud applications.

Supported Cloud application groups and applications will be maintained as a separate json file in Qosmos secpack. These applications groups are available only for casb configuration.

CASB policy rules will be enforced in order of configuration. Rules should be configured in the same order to bypass/allow specific match criteria for an application/activity and add a deny rule later to deny remaining cases.

**2.1  Goals**

N/a

**2.2  Exceptions**

**2.2.1  Caveats**

n/a

**2.2.2  Limitations**

CASB uses QOSMOS ixEngine to detect cloud application activities like login, upload and download. Bugs or limitations with Qosmos Engine on detecting the activities will be applied to CASB feature as well.

**2.2.3  Non-Goals**

**2.3  Assumptions**

**2.4  Functional competitive data**

N/A

**2.5  APIs/Messages**

N/A

**2.6  Manageability**

**2.6.1  CLI Config**

Examples:

Ø CASB policy to allow users to Share to Sharepoint application with given domain only

set security casb instance is1 application Sharepoint

set security casb instance is1 instance-id acmecorp07

set security casb instance is1 domain acmecorp07ms-my.sharepoint.com

set security casb instance is1 tag sanctioned

set security casb instance is1 type work

set security casb casb-policy casb-policy-1 rules rule1 match application Sharepoint activity Share param-name share-domain param-value acmecorp07

set security casb casb-policy casb-policy-1 rules rule1 match application Sharepoint instance is1

set security casb casb-policy casb-policy-1 rules rule1 then allow

set security casb casb-policy casb-policy-1 rules rule1 then log-action

set security casb casb-policy casb-policy-1 default-rule allow

set security casb casb-policy casb-policy-1 default-rule log-action

Ø CASB policy to deny download from all FireSharing applications

set security casb casb-policy casb-policy-2 rules rule1 match application-group FileSharing application any activity deny

set security casb casb-policy casb-policy-2 rules rule1 then deny

set security casb casb-policy casb-policy-1 default-rule allow

Apply CASB security Service

#set security policies from-zone trust to-zone untrust policy policy1 then permit application-services ?

Possible completions:

casb-policy CASB service (new addition to existing services)

#set security policies from-zone trust to-zone untrust policy policy1 then permit application-services casb-policy ?

Possible completions:

Specify CASB service profile name

**2.6.2  CLI Commands**

**2.6.2.1  CLI Command Details**

1. show security casb casb-policies

> Displays all casb-policies

2. show security casb casb-policies

> displays the configuration of CASB policy.

**2.6.2.2  JUNOScript**

**2.6.3  SNMP**

**2.6.4  Syslog – ERRMSG**

message CASB\_ACTION\_LOG {

required header msg\_header = 1;

optional string log\_tag = 2;

string source\_zone\_name = 3; /\* source\_zone \*/

optional string destination\_zone\_name = 4; /\* destination\_zone \*/

optional ipaddr source\_address = 5; /\* source\_address \*/

optional uint32 source\_port = 6; /\* source\_port \*/

optional ipaddr destination\_address = 7; /\* destination\_address \*/

optional uint32 destination\_port = 8; /\* destination\_port \*/

optional uint64 session\_id = 9; /\* session id \*/

optional string casb\_policy = 10; /\* casb policy name \*/

optional string rule\_name = 11; /\* rule matched \*/

optional string application = 12; /\* Cloud application \*/

optional string app\_user = 13; /\* application login user \*/

optional string activity = 14; /\* activity \*/

optional string action = 15; /action taken \*/

Optional string app\_instance=16; /Application instance \*/

Optional string casb-policy-name = 17 /\*casb policy name \*/

}

message CASB\_ACTIVITY\_LOG {

required header msg\_header = 1;

optional string log\_tag = 2;

string source\_zone\_name = 3; /\* source\_zone \*/

optional string destination\_zone\_name = 4; /\* destination\_zone \*/

optional ipaddr source\_address = 5; /\* source\_address \*/

optional uint32 source\_port = 6; /\* source\_port \*/

optional ipaddr destination\_address = 7; /\* destination\_address \*/

optional uint32 destination\_port = 8; /\* destination\_port \*/

optional uint64 session\_id = 9; /\* session id \*/

optional string application = 10; /\* application \*/

optional string app\_user = 11; /\* application user \*/

optional string activity = 12; /\* activity \*/

optional string app\_instance=13; /\*Application instance \*/

Optional string instance-domain=14 /\*Instance domain \*/

Optional string instance-tag=15 /\* Instance tag \*/

Optional string instance-type=16 /\*Instance type \*/

Optional string casb-policy-name = 17 /\* casb policy name \*/

Optional string casb-rule-name = 18 /\* casb rule name \*/

Optional string action = 19 /\*casb action \*/

}

**2.6.5  Software Feature Licensing**

NA

**2.6.6  Software Packaging**

Not Applicable

**2.6.7  J-Web Quick Configuration and Monitor Screen**

https://www.figma.com/file/I6R9OVtd4MS6reMAmj6k3z/CASB-Configuration?node-id=0:1

**2.6.8  Integration with Management Systems**

Not Applicable

**2.6.9  Telemetry**

Not Applicable

**2.6.10  JET API**

Not Applicable

**2.7  Examples or Interaction Descriptions**

**2.8  Supportability (Serviceability, Diagnose-ability and Fault Handling)**

**2.8.1  Serviceability and Diagnose-ability**

Using JDPI tracing for phase-1. Separate plug-in and debuggability will be added in phase-2

# RE traces enable:

set services application-identification traceoptions flag all

set services application-identification traceoptions file jdpi\_trace

set services application-identification traceoptions level

# PFE traces:

plugin casb set debug module

Flow. >> shows all packet path traces for CASB

Memory. >> memory reated traces

Pfeman >> ukern/policy load in PFE traces

# CASB stats:

plugin jdpi show casbstats

>> this command displays the CASB statistics: activity stats per application.

Plugin jdpi clear casbstats

>> this command clears the CASB statistics

**2.8.2  Fault Handling**

NA

**2.9  Dependencies and Interactions with other Components in the System**

**2.10  Legal Considerations**

**3  Topology Diagram**

# Include one or several topology diagrams used throughout sections 5, 6, 7. Provide pointer to file if external diagram file

Topology 1:

Proxy Server 8.0.0.1:3128

|

|

|ge-0/0/1

+------------------------+

Client1----------------|4.0.0.254/8 |

4.0.0.1 | SRX |ge-0/0/2

ge-0/0/0 | |--------------Internet

| Explicit Web Proxy |

Client2----------------| |

4.0.0.2 +------------------------+

Figure (1)

**4  DUT Configuration**

Refer https://systest.juniper.net/feature\_testplan/121741

**4.1  Test tool/ test equipment Configuration**

Operating System :

-----------------

Windows

Browsers :

----------

Chrome

**5  Feature verification: Test Methodology & Test Procedures**

Note :

Supported applications:

* Meta (Facebook) Messenger
* Office365\_Word
* Office365\_Excel
* Office365\_Powerpoint

ii. Basic Live testing to be checked

iii. Traffic : IPV4

iv. OS and Browsers : Mentioned in Section 4.

**5.1  Functional Testcases**

**Testcases**

**Tc5.1-1  Verify application - Meta (Facebook) Messenger and its activities - Login, Chat, FileTransfer and Audio/Video**

Procedure:

1. Configure CASB policy with the rule to hit MetaMessenger

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity Login

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity Chat

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity FileTransfer

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity Audio/Video

set security casb casb-policy cp1 rules r1 then allow

set security casb casb-policy cp1 rules r1 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to MetaMessenger beta user account

2. Start chat with alpha

3. Send files over the chat

4. Make an audio/video call

Verification:

1. Verify commit success

2. Check for syslog to get MetaMessenger activities, verify casb policy name, application name, rule name, action and activity

3. Check SSL proxy stats and RT\_FLOW logs

Login

Oct 1 03:14:23 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=49795 destination-address=163.70.138.9 destination-port=443 session-id=27124 application=METAMESSENGER username=unknown-user activity=login app-instance=NA instance-domain=NA instance-tag=NA instance-type=NA casb-policy-name=cp1 casb-rule-name=r14 casb-action=allow  
Oct 1 03:14:23 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=49795 destination-address=163.70.138.9 destination-port=443 session-id=27124 application=METAMESSENGER username=unknown-user activity=login app-instance=NA casb-policy-name=cp1

Chat  
Oct 1 03:14:27 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=49795 destination-address=163.70.138.9 destination-port=443 session-id=27124 application=METAMESSENGER username=unknown-user activity=chat app-instance=NA instance-domain=NA instance-tag=NA instance-type=NA casb-policy-name=cp1 casb-rule-name=r14 casb-action=allow  
Oct 1 03:14:27 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=49795 destination-address=163.70.138.9 destination-port=443 session-id=27124 application=METAMESSENGER username=unknown-user activity=chat app-instance=NA casb-policy-name=cp1

FileTransfer – Upload

Oct 1 03:15:21 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=49812 destination-address=163.70.138.9 destination-port=443 session-id=27159 application=METAMESSENGER username=unknown-user activity=filetransfer app-instance=NA instance-domain=NA instance-tag=NA instance-type=NA casb-policy-name=cp1 casb-rule-name=r14 casb-action=allow  
Oct 1 03:15:21 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=49812 destination-address=163.70.138.9 destination-port=443 session-id=27159 application=METAMESSENGER username=unknown-user activity=filetransfer app-instance=NA casb-policy-name=cp1

FileTransfer – Download

Oct 1 03:19:29 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=59454 destination-address=163.70.138.21 destination-port=443 session-id=27625 application=METAMESSENGER username=unknown-user activity=filetransfer app-instance=NA instance-domain=NA instance-tag=NA instance-type=NA casb-policy-name=cp1 casb-rule-name=r14 casb-action=allow  
Oct 1 03:19:29 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=59454 destination-address=163.70.138.21 destination-port=443 session-id=27625 application=METAMESSENGER username=unknown-user activity=filetransfer app-instance=NA casb-policy-name=cp1

FileTransfer – Image Download

root@aditya-appid-vsrx> show log messages|match casb   
Oct 4 06:43:36 aditya-appid-vsrx RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.12 source-port=50451 destination-address=157.240.23.25 destination-port=443 session-id=48327 application=METAMESSENGER username=unknown-user activity=filetransfer app-instance=NA instance-domain=NA instance-tag=NA instance-type=NA casb-policy-name=cp1 casb-rule-name=r14 casb-action=allow  
Oct 4 06:43:36 aditya-appid-vsrx RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.12 source-port=50451 destination-address=157.240.23.25 destination-port=443 session-id=48327 application=METAMESSENGER username=unknown-user activity=filetransfer app-instance=NA casb-policy-name=cp1

Audio/Video

Oct 1 03:26:19 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=49812 destination-address=163.70.138.9 destination-port=443 session-id=27159 application=METAMESSENGER username=unknown-user activity=audio/video app-instance=NA instance-domain=NA instance-tag=NA instance-type=NA casb-policy-name=cp1 casb-rule-name=r14 casb-action=allow  
Oct 1 03:26:19 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=49812 destination-address=163.70.138.9 destination-port=443 session-id=27159 application=METAMESSENGER username=unknown-user activity=audio/video app-instance=NA casb-policy-name=cp1

Audio/Video – Receive

root@aditya-appid-vsrx> show log messages|match casb   
Oct 11 03:55:08 aditya-appid-vsrx RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.12 source-port=59309 destination-address=163.70.138.9 destination-port=443 session-id=21189 application=METAMESSENGER username=unknown-user activity=audio/video app-instance=NA instance-domain=NA instance-tag=NA instance-type=NA casb-policy-name=cp1 casb-rule-name=r14 casb-action=allow  
Oct 11 03:55:08 aditya-appid-vsrx RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.12 source-port=59309 destination-address=163.70.138.9 destination-port=443 session-id=21189 application=METAMESSENGER username=unknown-user activity=audio/video app-instance=NA casb-policy-name=cp1

Platforms for Tc5.1-1:

* VSRX3.0

**Tc5.1-2  Verify application – MetaMessenger with instance and its activities**

Procedure:

1. Configure CASB policy with the rule to hit MetaMessenger

set security casb instance ins1 application MetaMessenger

set security casb instance ins1 instance-id acmecorp07

set security casb instance ins1 domain acmecorp07.com

set security casb instance ins1 tag sanctioned

set security casb instance ins1 type work

set security casb casb-policy cp1 rules r1 match application MetaMessenger instance ins1

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity Login

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity Chat

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity FileTransfer

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity Audio/Video

set security casb casb-policy cp1 rules r1 then allow

set security casb casb-policy cp1 rules r1 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to MetaMessenger beta user account

2. Start chat with alpha

3. Send files over the chat

4. Make an audio/video call

Verification:

1. Verify commit success

2. Check for syslog to get MetaMessenger activities, verify casb policy name, application name, rule name, action, app-instance, instance-domain, instance-tag, instance-type and activity

3. Check SSL proxy stats and RT\_FLOW logs

Platforms for Tc5.1-2:

* VSRX3.0

Source of requirement:

* undefined

**Tc5.1-3  Verify application - MetaMessenger** **with instance and its activities getting denied**

Procedure**:**

1. Configure CASB policy with the rule to hit MetaMessenger

set security casb instance ins1 application MetaMessenger

set security casb instance ins1 instance-id acmecorp07

set security casb instance ins1 domain acmecorp07.com

set security casb instance ins1 tag sanctioned

set security casb instance ins1 type work

set security casb casb-policy cp1 rules r1 match application MetaMessenger instance ins1

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity Login

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity Chat

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity FileTransfer

set security casb casb-policy cp1 rules r1 match application MetaMessenger activity Audio/Video

set security casb casb-policy cp1 rules r1 then deny

set security casb casb-policy cp1 rules r1 then log-action

set security casb casb-policy cp1 rules r2 match application MetaMessenger instance ins1

set security casb casb-policy cp1 rules r2 match application MetaMessenger activity Login

set security casb casb-policy cp1 rules r2 then deny

set security casb casb-policy cp1 rules r2 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to MetaMessenger and check if login in unsuccessful

5. Change deny action to allow for rule r1

6. Traffic

1. Login to MetaMessenger beta user account

2. Start chat with alpha

3. Send files over the chat

4. Make an audio/video call

Verification:

1. Verify commit success

2. Check for syslog to get MetaMessenger activities, verify MetaMessenger policy name, application name, rule name, action, app-instance, instance-domain, instance-tag, instance-type and activity

3. Verify if activities are getting denied as per the rules

4. Check SSL proxy stats and RT\_FLOW logs

Platforms for Tc5.1-3:

* VSRX3.0

**Tc5.1-4  Verify application - Office365\_Word and its activities - Open, AutoSave, SaveCopy, and Share**

Procedure:

1. Configure CASB policy with the rule to hit Office365\_Word

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity Open

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity AutoSave

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity SaveCopy

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity Share

set security casb casb-policy cp1 rules r1 then allow

set security casb casb-policy cp1 rules r1 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to Office365\_Word beta user account

2. Open a file

3. Edit file and check if its auto saved

4. Save a file

5. Share a file to alpha

Verification:

1. Verify commit success

2. Check for syslog to get Office365\_Word activities, verify casb policy name, application name, rule name, action and activity

3. Check SSL proxy stats and RT\_FLOW logs

Platforms for Tc5.1-4:

* VSRX3.0

**Tc5.1-5  Verify application – Office365 Word with instance and its activities**

Procedure:

1. Configure CASB policy with the rule to hit Office365\_Word

set security casb instance ins1 application Office365\_Word

set security casb instance ins1 instance-id acmecorp08

set security casb instance ins1 domain acmecorp08.com

set security casb instance ins1 tag sanctioned

set security casb instance ins1 type work

set security casb casb-policy cp1 rules r1 match application Office365\_Word instance ins1

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity Open

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity AutoSave

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity   
SaveCopy

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity Share

set security casb casb-policy cp1 rules r1 then allow

set security casb casb-policy cp1 rules r1 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to Office365\_Word beta user account

2. Open a file

3. Edit file and check if its auto saved

4. Save a file

5. Share a file to alpha

Verification:

1. Verify commit success

2. Check for syslog to get Office365\_Word activities, verify casb policy name, application name, rule name, action, app-instance, instance-domain, instance-tag, instance-type and activity

3. Check SSL proxy stats and RT\_FLOW logs

Open

Oct 1 02:41:01 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=60583 destination-address=13.107.138.10 destination-port=443 session-id=21719 application=OFFICE365\_WORD username=unknown-user activity=open app-instance=acmecorp08 instance-domain=acmecorp08.com instance-tag=work instance-type=NA casb-policy-name=cp1 casb-rule-name=r11 casb-action=allow  
Oct 1 02:41:01 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=60583 destination-address=13.107.138.10 destination-port=443 session-id=21719 application=OFFICE365\_WORD username=unknown-user activity=open app-instance=acmecorp08 casb-policy-name=cp1

AutoSave

Oct 1 02:42:53 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=52157 destination-address=52.108.9.12 destination-port=443 session-id=21758 application=OFFICE365\_WORD username=unknown-user activity=autosave app-instance=acmecorp08 instance-domain=acmecorp08.com instance-tag=work instance-type=NA casb-policy-name=cp1 casb-rule-name=r11 casb-action=allow  
Oct 1 02:42:53 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=52157 destination-address=52.108.9.12 destination-port=443 session-id=21758 application=OFFICE365\_WORD username=unknown-user activity=autosave app-instance=acmecorp08 casb-policy-name=cp1

SaveCopy

Oct 1 02:44:18 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=55779 destination-address=13.107.138.10 destination-port=443 session-id=22643 application=OFFICE365\_WORD username=unknown-user activity=savecopy app-instance=acmecorp08 instance-domain=acmecorp08.com instance-tag=work instance-type=NA casb-policy-name=cp1 casb-rule-name=r11 casb-action=allow  
Oct 1 02:44:18 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=55779 destination-address=13.107.138.10 destination-port=443 session-id=22643 application=OFFICE365\_WORD username=unknown-user activity=savecopy app-instance=acmecorp08 casb-policy-name=cp1

Share

Oct 1 02:47:52 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=61745 destination-address=13.107.138.10 destination-port=443 session-id=23029 application=OFFICE365\_WORD username=unknown-user activity=share app-instance=acmecorp08 instance-domain=acmecorp08.com instance-tag=work instance-type=NA casb-policy-name=cp1 casb-rule-name=r11 casb-action=allow  
Oct 1 02:47:52 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=61745 destination-address=13.107.138.10 destination-port=443 session-id=23029 application=OFFICE365\_WORD username=unknown-user activity=share app-instance=acmecorp08 casb-policy-name=cp1

Platforms for Tc5.1-5:

* VSRX3.0

Source of requirement:

* undefined

**Tc5.1-6  Verify application - Office365 Word with instance and its activities getting denied**

Procedure**:**

1. Configure CASB policy with the rule to hit Office365\_Word

set security casb instance ins1 application Office365\_Word

set security casb instance ins1 instance-id acmecorp08

set security casb instance ins1 domain acmecorp08.com

set security casb instance ins1 tag sanctioned

set security casb instance ins1 type work

set security casb casb-policy cp1 rules r1 match application Office365\_Word instance ins1

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity Open

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity AutoSave

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity   
SaveCopy

set security casb casb-policy cp1 rules r1 match application Office365\_Word activity Share

set security casb casb-policy cp1 rules r1 then deny

set security casb casb-policy cp1 rules r1 then log-action

set security casb casb-policy cp1 rules r2 match application Office365\_Word instance ins1

set security casb casb-policy cp1 rules r2 match application Office365\_Word activity Login

set security casb casb-policy cp1 rules r2 then deny

set security casb casb-policy cp1 rules r2 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to Office365\_Word and check if login in unsuccessful

5. Change deny action to allow for rule r1

4. Traffic:

1. Login to Office365\_Word beta user account

2. Open a file

3. Edit file and check if its auto saved

4. Save a file

5. Share a file to alpha

Verification:

1. Verify commit success

2. Check for syslog to get Office365\_Word activities, verify Office365\_Word policy name, application name, rule name, action, app-instance, instance-domain, instance-tag, instance-type and activity

3. Verify if activities are getting denied as per the rules

4. Check SSL proxy stats and RT\_FLOW logs

Platforms for Tc5.1-6:

* VSRX3.0

**Tc5.1-7  Verify application - Office365 Excel and its activities - Open, AutoSave, SaveCopy, and Share**

Procedure:

1. Configure CASB policy with the rule to hit Office365\_Excel

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity Open

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity AutoSave

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity SaveCopy

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity Share

set security casb casb-policy cp1 rules r1 then allow

set security casb casb-policy cp1 rules r1 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to Office365\_ Excel beta user account

2. Open a file

3. Edit file and check if its auto saved

4. Save a file

5. Share a file to alpha

Verification:

1. Verify commit success

2. Check for syslog to get Office365\_ Excel activities, verify casb policy name, application name, rule name, action and activity

3. Check SSL proxy stats and RT\_FLOW logs

Platforms for Tc5.1-7:

* VSRX3.0

**Tc5.1-8  Verify application – Office365 Excel with instance and its activities**

Procedure:

1. Configure CASB policy with the rule to hit Office365\_ Excel

set security casb instance ins1 application Office365\_ Excel

set security casb instance ins1 instance-id acmecorp08

set security casb instance ins1 domain acmecorp08.com

set security casb instance ins1 tag sanctioned

set security casb instance ins1 type work

set security casb casb-policy cp1 rules r1 match application Office365\_Excel instance ins1

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity Open

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity AutoSave

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity   
SaveCopy

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity Share

set security casb casb-policy cp1 rules r1 then allow

set security casb casb-policy cp1 rules r1 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to Office365\_ Excel beta user account

2. Open a file

3. Edit file and check if its auto saved

4. Save a file

5. Share a file to alpha

Verification:

1. Verify commit success

2. Check for syslog to get Office365\_ Excel activities, verify casb policy name, application name, rule name, action, app-instance, instance-domain, instance-tag, instance-type and activity

3. Check SSL proxy stats and RT\_FLOW logs

Open

"Oct 1 02:50:37 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=57672 destination-address=13.107.138.10 destination-port=443 session-id=23777 application=OFFICE365\_WORD username=unknown-user activity=open app-instance=acmecorp08 instance-domain=acmecorp08.com instance-tag=work instance-type=NA casb-policy-name=cp1 casb-rule-name=r11 casb-action=allow  
Oct 1 02:50:37 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=57672 destination-address=13.107.138.10 destination-port=443 session-id=23777 application=OFFICE365\_WORD username=unknown-user activity=open app-instance=acmecorp08 casb-policy-name=cp1

AutoSave

Oct 1 02:52:22 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=52372 destination-address=52.108.8.12 destination-port=443 session-id=23882 application=OFFICE365\_EXCEL username=unknown-user activity=autosave app-instance=acmecorp08 instance-domain=acmecorp08.com instance-tag=work instance-type=NA casb-policy-name=cp1 casb-rule-name=r13 casb-action=allow  
Oct 1 02:52:22 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=52372 destination-address=52.108.8.12 destination-port=443 session-id=23882 application=OFFICE365\_EXCEL username=unknown-user activity=autosave app-instance=acmecorp08 casb-policy-name=cp1

SaveCopy

Oct 1 02:53:33 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=52372 destination-address=52.108.8.12 destination-port=443 session-id=23882 application=OFFICE365\_EXCEL username=unknown-user activity=savecopy app-instance=acmecorp08 instance-domain=acmecorp08.com instance-tag=work instance-type=NA casb-policy-name=cp1 casb-rule-name=r13 casb-action=allow  
Oct 1 02:53:33 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=52372 destination-address=52.108.8.12 destination-port=443 session-id=23882 application=OFFICE365\_EXCEL username=unknown-user activity=savecopy app-instance=acmecorp08 casb-policy-name=cp1

Share

Oct 1 02:56:10 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=54470 destination-address=13.107.138.10 destination-port=443 session-id=24559 application=SHAREPOINT username=unknown-user activity=share app-instance=NA instance-domain=NA instance-tag=NA instance-type=NA casb-policy-name=cp1 casb-rule-name=default casb-action=allow  
Oct 1 02:56:10 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=54470 destination-address=13.107.138.10 destination-port=443 session-id=24559 application=SHAREPOINT username=unknown-user activity=share app-instance=NA casb-policy-name=cp1

Platforms for Tc5.1-8:

* VSRX3.0

Source of requirement:

* undefined

**Tc5.1-9  Verify application - Office365** **Excel** **with instance and its activities getting denied**

Procedure**:**

1. Configure CASB policy with the rule to hit Office365\_ Excel

set security casb instance ins1 application Office365\_ Excel

set security casb instance ins1 instance-id acmecorp08

set security casb instance ins1 domain acmecorp08.com

set security casb instance ins1 tag sanctioned

set security casb instance ins1 type work

set security casb casb-policy cp1 rules r1 match application Office365\_Excel instance ins1

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity Open

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity AutoSave

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity   
SaveCopy

set security casb casb-policy cp1 rules r1 match application Office365\_ Excel activity Share

set security casb casb-policy cp1 rules r1 then deny

set security casb casb-policy cp1 rules r1 then log-action

set security casb casb-policy cp1 rules r2 match application Office365\_ Excel instance ins1

set security casb casb-policy cp1 rules r2 match application Office365\_ Excel activity Login

set security casb casb-policy cp1 rules r2 then deny

set security casb casb-policy cp1 rules r2 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to Office365\_ Excel and check if login in unsuccessful

5. Change deny action to allow for rule r1

4. Traffic:

1. Login to Office365\_ Excel beta user account

2. Open a file

3. Edit file and check if its auto saved

4. Save a file

5. Share a file to alpha

Verification:

1. Verify commit success

2. Check for syslog to get Office365\_ Excel activities, verify Office365\_ Excel policy name, application name, rule name, action, app-instance, instance-domain, instance-tag, instance-type and activity

3. Verify if activities are getting denied as per the rules

4. Check SSL proxy stats and RT\_FLOW logs

Platforms for Tc5.1-9:

* VSRX3.0

**Tc5.1-10  Verify application - Office365 Powerpoint and its activities - Open, AutoSave, SaveCopy, and Share**

Procedure:

1. Configure CASB policy with the rule to hit Office365\_Powerpoint

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity Open

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity AutoSave

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity SaveCopy

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity Share

set security casb casb-policy cp1 rules r1 then allow

set security casb casb-policy cp1 rules r1 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to Office365\_ Powerpoint beta user account

2. Open a file

3. Edit file and check if its auto saved

4. Save a file

5. Share a file to alpha

Verification:

1. Verify commit success

2. Check for syslog to get Office365\_ Powerpoint activities, verify casb policy name, application name, rule name, action and activity

3. Check SSL proxy stats and RT\_FLOW logs

Platforms for Tc5.1-10:

* VSRX3.0

**Tc5.1-11  Verify application – Office365 PowerPoint with instance and its activities**

Procedure:

1. Configure CASB policy with the rule to hit Office365\_ Powerpoint

set security casb instance ins1 application Office365\_ Powerpoint

set security casb instance ins1 instance-id acmecorp08

set security casb instance ins1 domain acmecorp08.com

set security casb instance ins1 tag sanctioned

set security casb instance ins1 type work

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint instance ins1

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity Open

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity AutoSave

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity SaveCopy

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity Share

set security casb casb-policy cp1 rules r1 then allow

set security casb casb-policy cp1 rules r1 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to Office365\_ Powerpoint beta user account

2. Open a file

3. Edit file and check if its auto saved

4. Save a file

5. Share a file to alpha

Verification:

1. Verify commit success

2. Check for syslog to get Office365\_ Powerpoint activities, verify casb policy name, application name, rule name, action, app-instance, instance-domain, instance-tag, instance-type and activity

3. Check SSL proxy stats and RT\_FLOW logs

Open

Oct 1 03:00:06 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=63287 destination-address=13.107.138.10 destination-port=443 session-id=25211 application=OFFICE365\_POWERPOINT username=unknown-user activity=open app-instance=acmecorp08 instance-domain=acmecorp08.com instance-tag=work instance-type=NA casb-policy-name=cp1 casb-rule-name=r12 casb-action=allow  
Oct 1 03:00:06 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=63287 destination-address=13.107.138.10 destination-port=443 session-id=25211 application=OFFICE365\_POWERPOINT username=unknown-user activity=open app-instance=acmecorp08 casb-policy-name=cp1

AutoSave

Oct 1 03:06:17 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=63294 destination-address=52.108.8.12 destination-port=443 session-id=25223 application=OFFICE365\_POWERPOINT username=unknown-user activity=autosave app-instance=NA instance-domain=NA instance-tag=NA instance-type=NA casb-policy-name=cp1 casb-rule-name=default casb-action=allow  
Oct 1 03:06:17 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=63294 destination-address=52.108.8.12 destination-port=443 session-id=25223 application=OFFICE365\_POWERPOINT username=unknown-user activity=autosave app-instance=NA casb-policy-name=cp1

SaveCopy  
Oct 1 03:06:46 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=63294 destination-address=52.108.8.12 destination-port=443 session-id=25223 application=OFFICE365\_POWERPOINT username=unknown-user activity=savecopy app-instance=NA instance-domain=NA instance-tag=NA instance-type=NA casb-policy-name=cp1 casb-rule-name=default casb-action=allow  
Oct 1 03:06:46 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=63294 destination-address=52.108.8.12 destination-port=443 session-id=25223 application=OFFICE365\_POWERPOINT username=unknown-user activity=savecopy app-instance=NA casb-policy-name=cp1

Share

Oct 1 03:09:50 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTION\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=56101 destination-address=13.107.138.10 destination-port=443 session-id=26431 application=OFFICE365\_POWERPOINT username=unknown-user activity=share app-instance=acmecorp08 instance-domain=acmecorp08.com instance-tag=work instance-type=NA casb-policy-name=cp1 casb-rule-name=r12 casb-action=allow  
Oct 1 03:09:50 idpdevesx8-vsrx3-10 RT\_CASB: CASB\_ACTIVITY\_LOG: source-zone-name=untrust destination-zone-name=trust source-address=4.0.0.27 source-port=56101 destination-address=13.107.138.10 destination-port=443 session-id=26431 application=OFFICE365\_POWERPOINT username=unknown-user activity=share app-instance=acmecorp08 casb-policy-name=cp1

Platforms for Tc5.1-11:

* VSRX3.0

Source of requirement:

* undefined

**Tc5.1-12  Verify application - Office365 PowerPoint with instance and its activities getting denied**

Procedure**:**

1. Configure CASB policy with the rule to hit Office365\_ Powerpoint

set security casb instance ins1 application Office365\_ Powerpoint

set security casb instance ins1 instance-id acmecorp08

set security casb instance ins1 domain acmecorp08.com

set security casb instance ins1 tag sanctioned

set security casb instance ins1 type work

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint instance ins1

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity Open

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity AutoSave

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity SaveCopy

set security casb casb-policy cp1 rules r1 match application Office365\_ Powerpoint activity Share

set security casb casb-policy cp1 rules r1 then deny

set security casb casb-policy cp1 rules r1 then log-action

set security casb casb-policy cp1 rules r2 match application Office365\_ Powerpoint instance ins1

set security casb casb-policy cp1 rules r2 match application Office365\_ Powerpoint activity Login

set security casb casb-policy cp1 rules r2 then deny

set security casb casb-policy cp1 rules r2 then log-action

2. Configure CASB policy default rule

set security casb casb-policy cp1 default-rule deny

3. Associate CASB policy to firewall policy

set security policies from-zone untrust to-zone trust policy 1 then permit application-services casb-policy cp1

4. Traffic:

1. Login to Office365\_ Powerpoint and check if login in unsuccessful

5. Change deny action to allow for rule r1

4. Traffic:

1. Login to Office365\_ Powerpoint beta user account

2. Open a file

3. Edit file and check if its auto saved

4. Save a file

5. Share a file to alpha

Verification

1. Verify commit success

2. Check for syslog to get Office365\_ Powerpoint activities, verify Office365\_ Powerpoint policy name, application name, rule name, action, app-instance, instance-domain, instance-tag, instance-type and activity

3. Verify if activities are getting denied as per the rules

4. Check SSL proxy stats and RT\_FLOW logs

Platforms for Tc5.1-12:

* VSRX3.0

**Test Matrix**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Testname** | **Type** | **Commitment** | **Scriptable** | **Scripted** | **Manual Regression** | **Platforms** |
| Tc 5.1-1: Verify application - Meta (Facebook) Messenger and its activities - Login, Chat,  FileTransfer and Audio/Video | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |
| Tc 5.1-2: Verify application – MetaMessenger with instance and its activities | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |
| Tc 5.1-3: Verify application – MetaMessenger with instance and its activities getting denied | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |
| Tc 5.1-4: Verify application - Office365\_Word and its activities - Open, AutoSave, SaveCopy, and Share | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |
| Tc 5.1-5: Verify application – Office365 Word with instance and its activities | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |
| Tc 5.1-6: Verify application - Office365 Word with instance and its activities getting denied | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |
| Tc 5.1-7: Verify application - Office365 Excel and its activities - Open, AutoSave, SaveCopy, and Share | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |
| Tc 5.1-8: Verify application – Office365 Excel with instance and its activities | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |
| Tc 5.1-9: Verify application - Office365  Excel with instance and its activities getting denied | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |
| Tc 5.1-10: Verify application - Office365 Powerpoint and its activities - Open, AutoSave, SaveCopy, and Share | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |
| Tc 5.1-11: Verify application – Office365 PowerPoint with instance and its activities | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |
| Tc 5.1-12: Verify application - Office365 PowerPoint with instance and its activities getting denied | Basic | 21.2X32D30 | N (manual) | N | VSRX3.0 |  |

**Test Result Matrix**

**Execution List**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Execution Number** | **Date/Time** | **Milestone** | **Type** | **Log** | **Notes** |

| **Testcase** | **Scenario** |
| --- | --- |
| 5.1-1 | default |
| 5.1-2 | default |
| 5.1-3 | default |
| 5.1-4 | default |
| 5.1-5 | default |
| 5.1-6 | default |
| 5.1-7 | default |
| 5.1-8 | default |
| 5.1-9 | default |
| 5.1-10 | default |
| 5.1-11 | default |
| 5.1-12 | default |