

Edge Firewall ATP services (IDS/IPS, URLF, Reputation)

VeloCloud Products

Exported on 11/20/2024

Table of Contents

1	PRD SIGN-OFF	4
2	1.0 Feature Description	6
3	2.0 Objective.....	7
4	3.0 User Stories.....	8
5	3.1 Feature Support	9
6	3.3 VCE Firewall ATP Packages / License	11
7	5.0 Impact.....	12
8	6.0 Requirements.....	13
9	6.1 Tenant Provisioning Requirements	14
10	6.2 ATP Service Deployments.....	15
11	6.3 ATP Security Requirements	17
11.1	6.3.1 IDS/IPS, Reputation & Threat Intelligence.....	17
11.2	6.3.2 URL Filtering.....	22
12	6.4 Management Plan Requirements	30
12.1	6.4.2 URL Filtering.....	30
13	7.0 Logging, Reporting, Alarm, and Troubleshooting	35
14	8.0 Performance and Scale Requirements.....	42
15	9.0 Open Questions	43
16	10.0 Out of Scope	44
17	Edge Firewall ATP Services - SASE SE/SA Feedback.....	45
18	Sept. 16 Meeting Notes with Tom Speeter	48
19	VCE Enhanced Firewall Services - PM/Dev/TME/UX Weekly Sync	49
19.1	Yamazaki Release Open Issues	49
19.1.1	Yamazaki FW Feature Target List & Status - List of features targeted for Yamazaki including status for PRD, UX, FS approvals.	53
19.2	Woodford Release Open Issues.....	53
19.3	PRD Review Meetings.....	56

19.4	Weekly Engineering/Product Sync Meetings (Internal).....	58
19.5	UX VCE ATP Features Workshop (May 9th, 2022)	63
19.6	Parking Lot Questions	63

1 PRD SIGN-OFF

Target release	WOODFORD (IDS/IPS) YAMAZAKI (URLF, Reputation)
Sign-Off Date	October 20, 2022 (Woodford) March 30, 2023 (Yamazaki)
Epic	VLENG-97334 ¹ (IDS/IPS) VLENG-1219074 ³ (URLF & Reputation) VLENG-4132732 ⁵ (Monitoring: URLF & Reputation)
Document status	APPROVED
Document owner	@Sathya Thammanur
Architect	@Gurudutt Maiya Belur
MP Owner	@Aditya Agarwal
DP Owner	@Unknown User (sapk) @Unknown User (saravanank)
QA Owner	@Sivabalan Pandian
UX Owner	@Ritesh Tiwari
System Owner	

1 <https://jira.eng.vmware.com/browse/VLENG-97334>

2 <https://jira.eng.vmware.com/browse/VLENG-97334>

3 <https://jira.eng.vmware.com/browse/VLENG-119074>

4 <https://jira.eng.vmware.com/browse/VLENG-97334>

5 <https://jira.eng.vmware.com/browse/VLENG-132732>

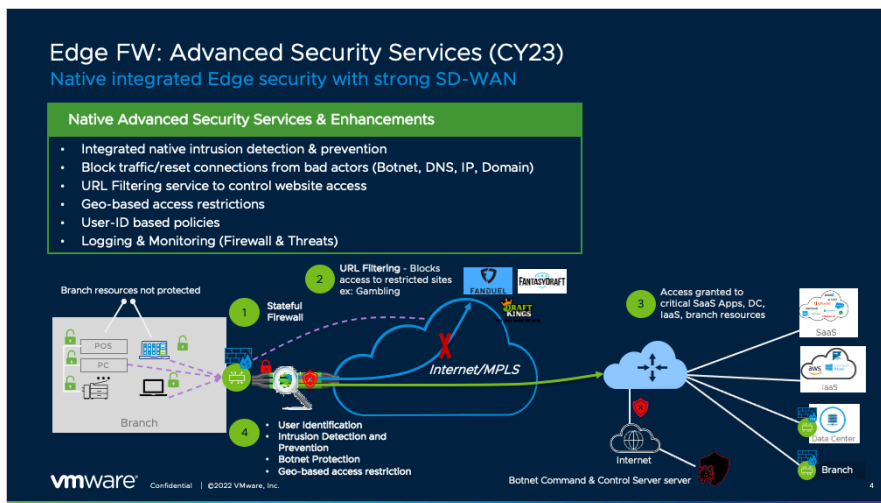
Tech Ops	<Tech Ops Owner>
----------	------------------

2 1.0 Feature Description

Advanced threat protection (ATP) service is an undertaking to provide ATP functions on VCE Edges. The ATP (Advanced Threat Protection) functionality will be powered by NSX technology. The ATP service will support protecting VCE traffic from intrusions across branch 2 branch, branch 2 hub or branch to internet traffic patterns. The NSX powered ATP functionality shall include IDS/IPS, Reputation & Threat Intelligence and URL Filtering security services. [An end customer configures and manages the ATP services via Firewall functionality in VCO.](#)

3 2.0 Objective

Currently, VCE FW provides stateful inspection along with application identification without additional ATP security features. While the stateful FW of VCE provides security, it is not adequate and creates a gap in providing ATP security integrated natively with SDWAN. Edge Firewall ATP services goal is to address these security gaps and offer advanced threat protection natively on the edge in conjunction with SDWAN. The solution is a significant initiative both in terms of customer retention (SD-WAN customers looking for integrated advanced security solutions) and market expansion.



The ATP feature set will be launched in multiple phases.

The MVP for the first launch targeted for Woodford is available in this deck. ⁶

⁶ https://onevmw.sharepoint.com/:p:/t/velo-products/EUTzLfRPMKNJiqdJ5D9agaQBC7y_WiqX6AqePAnEKm3s-g?e=utaAPa

4 3.0 User Stories

Please list out the user stories. Examples below:

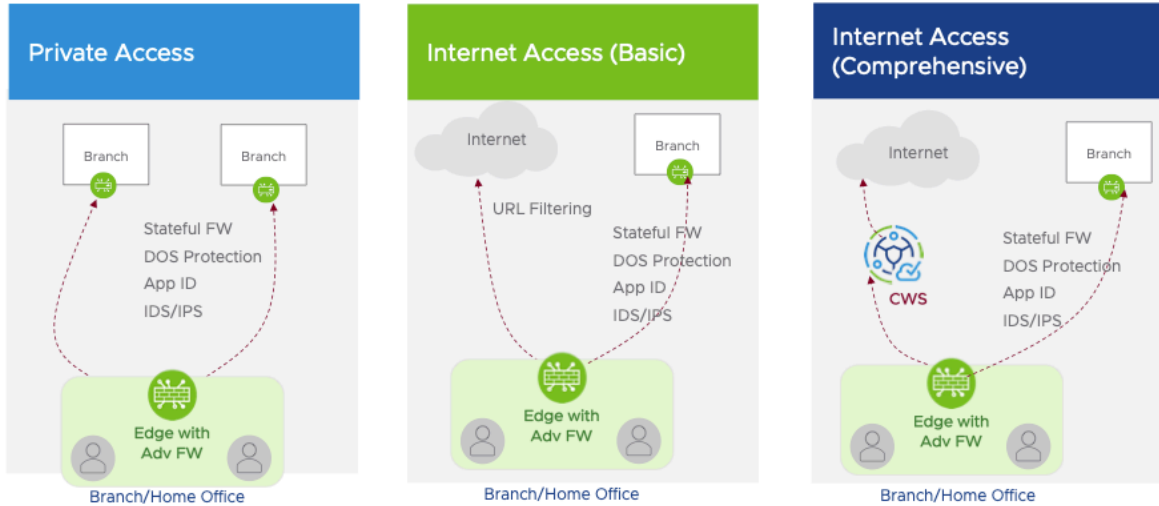
#	User Story	Priority	ETA	Engineering Response	
				V el o	N S X
1	Private Access: Branch user is able to access resources in branch (intra-branch and inter-branch) w/security protections (ATP): <ul style="list-style-type: none"> • IDS/IPS • Reputation & threat intelligence • URL Filtering Lite (SNI based filtering for HTTPS) Note: Internet bound web traffic on standard ports (80/443) through the gateway should continue to be routed to CWS for inspection to avail services including SSL Decryption, Sandboxing and Anti-malware.	High	WOODFORD		
2	Private Access: Branch access user is able to access resources in IaaS (AWS, GCP, VMC, etc.) w/security protections (see (UC#1 for list)	Medium	WOODFORD		
3	Private Access: Branch access user is able to access resources in DC w/ security protections (see (UC#1 for list).	Low	Phase 2		
4	Internet Access: Branch user is able to access internet applications w/security protections (ATP): <ul style="list-style-type: none"> • IDS/IPS • Reputation & threat intelligence • URL Filtering Lite (SNI based filtering for HTTPS) Note: Internet bound web traffic on standard ports (80/443) through the gateway should continue to be routed to CWS for inspection to avail services including SSL Decryption, Sandboxing and Anti-malware.	High	WOODFORD		

5 3.1 Feature Support

#	Phase	User Story	ATP Function
1	1	Block known malicious sites & Command-and-Control callbacks traffic from infecting end user devices and enterprise networks by using database of known bad IP's, DNS domains & URLs.	Reputation & Threat Intelligence
2	1	Detect and prevent known exploits triggering vulnerability in software from entering network.	IDS/IPS
3	1	Protect users behind edge against websites spreading malware, stealing information, hosting inappropriate content	URL Filtering
4	2	Detect anomalous activity and malicious behavior & provide high fidelity insights into advanced threats entering into user network	Network Traffic Analysis
5	1	Provide logs of all allowed/denied traffic as per the firewall policy	Logging
6	1	Provide monitoring dashboard for threat and traffic analysis	Monitoring
7	2	Provide Geo-based restriction of inbound/outbound traffic via edges	Geo-based access control
8	2	Provide user level visibility of traffic for branch access. Provide ability to limit user/user group access to applications/resources through integration with prominent identity solutions.	User Identity

Edge ATP Firewall – Use Cases

Expanding security for internal and simple internet branch access use cases



6 3.3 VCE Firewall ATP Packages / License

ATP service will be offered as a single add-on license supporting all SDWAN packages. Support for the ATP service license must be made available at the first launch planned for Woodford. Bundling of ATP service with SDWAN packages (Enterprise/Premium is currently under investigation as part of Pricing-n-Packaging (PnP) effort. Details of PnP will be added to this PRD once the packaging is finalized.

4.0 Assumptions

7 5.0 Impact

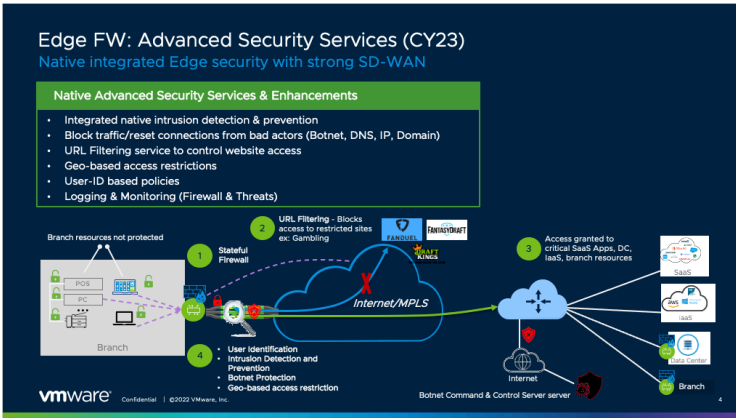
Impact	Response	Comments
DP Documentation	<input checked="" type="checkbox"/> User Guide <input type="checkbox"/> DP Monitoring <input type="checkbox"/> No Doc Required	
MP Documentation	<input checked="" type="checkbox"/> User Guide <input type="checkbox"/> MP Monitoring <input type="checkbox"/> No Doc Required	
Platform Documentation	<input checked="" type="checkbox"/> User Guide <input type="checkbox"/> No Doc Required	
Feature Flag	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
TechOps Impact (Architecture Changes?)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not Sure	

8 6.0 Requirements

9 6.1 Tenant Provisioning Requirements

#	Requirements	Importance	ETA	Jira	Eng. Reponse
Tenant 6.1.1	<p>ATP services should be controlled by customer capabilities flags which will eventually be turned on based on the license.</p> <p>Single bundle: Includes Reputation & Threat Intelligence, IDS/IPS, URL Filtering</p>	HIGH	WOODFORD		

10 6.2 ATP Service Deployments

#	Requirements	Importance	ETA	Jira Issue
ATPD 1.1	<p>Native Edge Integration</p> <p>ATP services must be natively integrated with the firewall engine in the SDWAN Edges.</p>  <p>Edge FW: Advanced Security Services (CY23) Native integrated Edge security with strong SD-WAN</p> <p>Native Advanced Security Services & Enhancements</p> <ul style="list-style-type: none"> Integrated native intrusion detection & prevention Block traffic/reset connections from bad actors (Botnet, DNS, IP, Domain) URL Filtering service to control website access Geo-based access restrictions User-ID based policies Logging & Monitoring (Firewall & Threats) <p>Branch resources not protected</p> <p>1. User behind the edge sends traffic to Internet/SaaS/Private applications</p> <p>2. Traffic sent/received through the VCE is subject to the business/security policy (with IDS/IPS, Botnet, URLF)</p> <p>3. Based on the security policy (firewall, IDS/IPS, Botnet, URLF) traffic is inspected by the firewall engine & the ATP engine, content is matched against signatures configured in the ATP engine</p> <p>a. If no attack is detected, then the ATP engine forwards the traffic to the client</p>	HIGH	WOOD FORD YAMA ZAKI	

#	Requirements	Importance	ETA	Jira Issue
ATPD 1.2	High Availability ATP must support stateful high availability and must have the following capabilities <ul style="list-style-type: none"> • Stateful session sync between two nodes in legacy and enhanced HA modes. • ATP flows sync between active/standby nodes (unless there is a technical limitation on the suricata library, this needs to be a high priority to avoid security vulnerability on ATP flow restart) • Security policy sync including Firewall rules and ATP settings • Maintain same version of ATP engine (which is tied to the edge firmware) and signature set • Stateful failover from one node to another WITHOUT traffic disruption 	HIGH	WOOD FORD	
ATPD 1.3	Hosting of VMWare Signature Database (VMware ATP Database) VMware must host and maintain the signature Database for ATP (IDS/IPS, Reputation, URLF). This database must be in sync with the external signature providers like Trustwave, Webroot and Dell Secure Works ATP engine in the SDWAN edges connect to VCO via a secure channel (same as used for edge config and firmware upgrades today) and get the updates for the IDS/IPS, Reputation, URLF engine and signature packs. Hosted VMware ATP Database must provide following capabilities <ul style="list-style-type: none"> • Provide the updates to the IPS, Reputation, URLF engine • Provide latest signature packs • Sync with the external signature sources • Must support hitless upgrade of signatures 	HIGH	WOOD FORD YAMA ZAKI	

11 6.3 ATP Security Requirements

11.1 6.3.1 IDS/IPS, Reputation & Threat Intelligence

Requirement Number	Description	Priority	ETA	Jira Issue	Engineering Responses
	Signature-based detection and prevention				NSX
IPS 1.1	<p>IPS Engine</p> <p>IPS Engine is the core processing module of the IPS solution. It performs the following actions</p> <p>Inspect traffic/transaction → Decode Application → Extract Content → Match Signature → Take Action</p> <p>NSX IPS uses the open-source IPS Engine called "Suricata". The solution must continue to use the same engine developed by the NSX IPS team</p> <p>https://suricata-ids.org/</p>	HIGH	WOO DFOR D		
IPS 1.2	<p>Supported Protocols</p> <p>IPS engine must recognize, decode and extract content from the following applications</p> <ul style="list-style-type: none"> • HTTP Applications: All web applications • HTTPS Applications: All web applications (as supported by the Suricata library without decryption requirements) • POP3 / IMAP / SMTP: Mail traffic • FTP: File transfers • SMB: Samba • DNS • L3 / L4 Applications: RTP 	HIGH	WOO DFOR D		

IPS 1.3	Packaging of IPS Engine IPS Engine is packaged along with the SDWAN base image. There is no separate base package available for the IPS Engine. However, the updates to the IPS signatures can be done in real-time, IPS signature update must not require updating the SDWAN base image/ operating system.	HIGH	WOO DFOR D		
IPS 1.4	IPS for GZIP traffic To extract content from the GZIP traffic, the IPS engine must decode the GZIP type and decompress it and apply the IPS policy and compress it back before forwarding traffic Traffic → IPS Engine (Decode ZIP Type -- Decompress -- Apply Policy -- Compress) → Traffic	HIGH	XANT E+		
IPS 1.5	IPS for Tunneled Traffic IPS Engine must recognize common tunnel protocols and extract content from the tunnel protocols. IPS Engine must support the following tunnel protocols <ul style="list-style-type: none"> • GRE • VXLAN • IP-IP 	HIGH	YAM AZAK I+		

IPS 1.6	<p>IPS & Reputation Signatures</p> <p>Signature is a pattern represented by the attack or vulnerability exploitation. IPS Engine matches the signature against the traffic payload and decides whether it is an attack or not.</p> <p>The solution must support more than 20,000 signatures, by default the SDWAN base image does not have signatures. Once the IPS policy is configured the ATP system in the SDWAN Edge will download the latest signature pack and install it to the local system. Support must be provided to ensure signatures be optimized for space to support low end vs. mid/high end edge devices. For example, low end edges can support signatures for last 6 months vs. mid/high end provides signatures to cover longer time duration (last 1Yr+).</p> <p>Signatures must support to the following</p> <ul style="list-style-type: none"> • Signatures to detect and prevent traffic trying to exploit known vulnerabilities • Signatures to detect and prevent command-and-control traffic in DNS tunnel or other disguising protocols • Signatures on ZIP/GZIPd files • Signatures on tunneled traffic • Automatic signature updates 	HIGH	<p>WOO DFOR D</p> <p>YAM AZAK I (Reput ation)</p>		
IPS 1.7	<p>Reputation based blocking</p> <p>IP denylist to block traffic going to known bad actors</p>	HIGH	YAM AZAK I		
IPS 1.8	<p>Signature Sources</p> <p>The efficacy of the IPS solution is depended on the quality of the signatures. IPS solution must have signatures to detect attacks seen in the last 10-12 years. Also, it must keep up to date with the latest attacks and acquire a signature for it.</p> <p>There are numerous commercial and community-based signature offerings existed in the market. Leverage the signature sources as supported by the NSX IPS Solution for VMware SD-WAN ATP engine.</p>	MEDI UM	WOO DFOR D		
IPS 1.9	<p>Custom Signatures</p> <p>The solution must allow the customer admin / Sec Ops team to create their signatures. Signatures can be created in YAML or XML format</p>	LOW	YAM AZAK I+		

IPS 1.10	Secure Connection to the VMware IPS Database The system must create a secure communication to hosted VMware IPS Database and use strong encryption while downloading signature packs	HIGH	WOODFORD		
IPS 1.11	Updating IPS Engine The system must support updating the IPS engine similar to the updates done for SDWAN Edge system image. IPS Engine (suricata library) must be kept in sync with the NSX solution; if the local version is lower than the NSX version, the system generates a new SDWAN Edge image with the new changes.	HIGH	WOODFORD		
IPS 1.12	Updating IPS Signature The system must support updating the Signatures WITHOUT requiring an update to the base SDWAN Edge system image or the IPS engine. The system must poll the cloud-hosted database (VMware IPS Database), if the local sig-pack version is lower than the cloud version, the system downloads the signature updates and re-load with new changes. The poll timer is defined and not configurable.	HIGH	WOODFORD		
IPS 1.13	Offline Updates The system must provide an option to update the IPS signature offline. This option is only available to the Cloud / Tech Ops. Admins must be able to download the latest sig-packs, and update VCO manually. Manual updates should be done at the VCO level. For Xante, the updates from VCO to edge will be automatic and follow same behavior as the VMW hosted solution. Scheduling of signature updates can be planned for future when VMW hosted solution can support the feature.	MEDIUM	YAMAZAKI+		
	IDPS enforcement				
IPS 1.9	Option to run either in detection mode or prevention mode (default is to do IDPS)	MEDIUM	WOODFORD		

	IDPS & Reputation Security Configuration Options				
IPS 1.10	Provide ability to configure IDS / IPS functionality based on severity levels as defined by NSX Signature database	MEDIUM	YAM AZAK I+		
IPS 1.11	Provide user to configure IDS / IPS functionality as an object group listed under Security → Security Services. Refer to slides ⁷ for details.	HIGH	YAM AZAK I		
IPS 1.12	Allow users to choose a default IDS/IPS object group or any of user defined IDS/IPS object group as part of Firewall rule creation. Refer to slides ⁸ for details.	HIGH	YAM AZAK I		
IPS 1.13	Provide ability to configure IP Reputation functionality (exposed as Malicious IP Filtering) based of reputation categories as defined by NSX Malicious IP database. Refer to slides ⁹ for details.	HIGH	YAM AZAK I		
IPS 1.14	Provide user to configure Malicious IP functionality as an object group listed under Security → Security Services. Refer to slides ¹⁰ for details.	HIGH	YAM AZAK I		
IPS 1.15	Allow users to choose a default Malicious IP object group or any of user defined Malicious IP object group as part of Firewall rule creation. Refer to slides ¹¹ for details.	HIGH	YAM AZAK I		

⁷ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

⁸ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

⁹ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

¹⁰ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

¹¹ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

11.2 6.3.2 URL Filtering

Requirement Number	Description	Priority	ETA	Jira Issue	Engineering Responses
	Dataplane processing				
URL 1.1	<p>URL Filtering</p> <p>For every incoming HTTP REQUEST packets, the Edge platform must extract the URL from the HTTP packets and categorize the URL (e.g., www.cnn.com¹² is a News category). Then the “allow,” “drop” and “reject” decision is made based on the URL category. A sample sequence of activities at the Edge is defined in the below figure</p> <pre> graph TD Start([User behind the Edge, opens browser and type www.google.com]) --> Recv[HTTP request packets received at the Edge] Recv --> Buffer{Edge buffer the HTTP requests and extract URL from the packets} Buffer --> Cache{Is URL category information available in Cache} Cache -- Yes --> Policy{Policy lookup for the category} Policy -- Allowed --> Forward([Forward the HTTP request to the Web Server; No further action]) Policy -- Drop / Reject --> Block([Send block page as a response to the HTTP request if action is Reject, otherwise silent drop]) Cache -- No --> SendDB[Send URL to VMW Hosted Categorization Database for categorization] SendDB --> RecvDB[VMW Categorization Database send back category of the URL] RecvDB --> CacheURL([Cache URL and its category]) CacheURL --> Policy </pre> <p>For cache miss on local database lookup, the url will be classified as unknown category and action will be taken based on the definition for unknown categories. Query for URL category will happen asynchronously to not impact performance.</p>	HIGH	YAMA ZAKI		

¹² <http://www.cnn.com/>

URL 1.2	HTTP Protocols Support The solution must intercept and extract URL information from the HTTP methods – GET, POST, PUT, HEAD, OPTIONS, TRACE, DELETE, CONNECT	HIGH	YAMA ZAKI		
URL 1.3	HTTPS Traffic Support using SNI In the HTTPS packets, the URL information is encrypted, and it is challenging to extract the URL information from the HTTP payload without Edge acting as SSL Forward Proxy (SSL man-in-middle). Implementing and configuring the SSL proxy is not trivial. Instead, Edge platforms must snoop the SSL transaction between client and server, the SNI field in the SSL transaction provides the URL information. So, by extracting the URL information from the SNI field, the Edge platform will be able to identify the URL category	HIGH	YAMA ZAKI		
URL 1.4	URL Filtering for Underlay and Overlay Traffic URL filtering must support on the traffic going over <ul style="list-style-type: none"> • DMPO • non DMPO tunnels • Direct internet access WAN links (underlay) 	HIGH	YAMA ZAKI		
	URL Groups & Categories				
URL 1.5	URL Group URL Group is an object with a set of URL categories. A URL Group can contain the pre-defined URL categories and custom URL List. Admins can create multiple URL Groups, but only one URL Group can be referenced in one single firewall policy. A new tab must be added to the Object Groups page for the URL Groups under Security section. Refer to slides ¹³ for details. A new "URL Group" must-have the following sections - Reputation List, Custom URL List and Pre-defined URL Categories (arranged in alphabet order). Admin can add URLs to the Custom URL List OR select one or more pre defined URL categories into the URL Groups.	HIGH	YAMA ZAKI		

¹³ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

URL 1.6	<p>Pre-defined URL Categories</p> <p>There are hundreds of millions of websites and URLs. It is very tedious to configure the policy for individual URLs, so these URLs are mapped to a specific category, and then filtering policy is applied over the categories.</p> <p>Every URL is mapped to the specific URL category (e.g. www.cnn.com¹⁴ is part of the news category). Except for the custom URL list, all of the URL Filtering policy decision is based on the URL category</p> <p>The number of URL Categories on the Edge platforms must be the same as in the Cloud-hosted Categorization Database, which in turn should match the Webroot database.</p> <p>As per the Webroot datasheet, Webroot has 10 URL Category Groups and 80 URL Categories.</p>	HIGH	YAMA ZAKI		
URL 1.7	<p>Web / IP Reputation</p> <p>Web / URL reputation provides the trustworthiness of the Web site. Most popular URL Filtering solution (like Webroot) track the websites overtime for the malicious and inappropriate content and assign a score between 0 to 100.</p> <ul style="list-style-type: none"> • 81-100: Trustworthy • 61-80: Low risk • 41-60: Moderate risk • 21-40: Suspicious • 01-20: High risk <p>VMware solution must include this reputation score in the policy decision. Please refer REQ#URL 1.9 for details on how Web / IP Reputation is included in the policy decision</p>	MEDI UM	XANT E+		

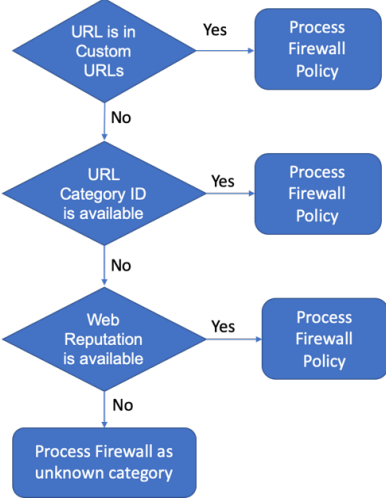
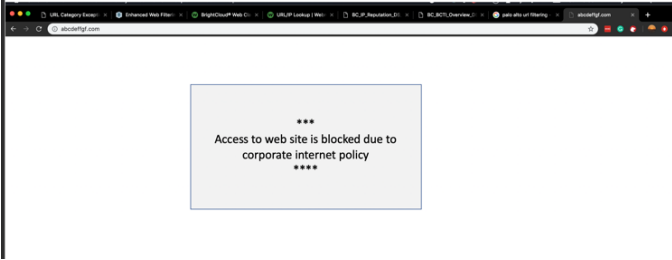
¹⁴ <http://www.cnn.com/>

URL 1.8	<p>Custom URL List</p> <p>Many times, admin wants to allow / drop / reject specific sites independent of their categories (Whitelisting of URLs/Domains), and they will be able to do so by adding those URLs in the "custom URL List" section</p> <p>Admins must be able to add the wildcards, regular expression patterns in the custom URL List.</p> <p>Object Groups → URL Groups → New Edit URL Group → Add URLs in the Custom URL List sections</p> <p>Characters "." "/" "?" "&" "=" ";" "+" in the URL are considered as a separator, every string separated by one or two of these characters is a token. Wildcard character "*" is used as a replacement to the token.</p> <p>Valid URL patterns:</p> <ul style="list-style-type: none"> • *.yahoo.com¹⁵ • www.*.com • www.vmware.* <p>Invalid URL patterns</p> <ul style="list-style-type: none"> • ww*.yahoo.com¹⁶ • www.vm*ware.com¹⁷ <p>For Xante, it is acceptable to support the whitelisting of URL/Domains. Wildcard support can be done post Xante release.</p>	MEDI UM	YAMA ZAKI		
---------	--	------------	--------------	--	--

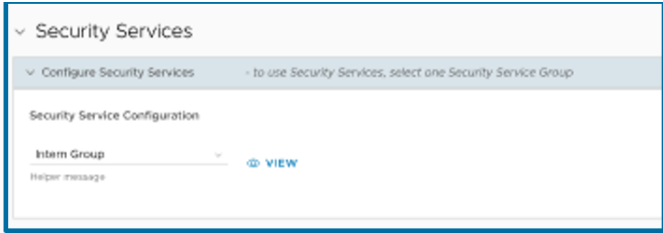
¹⁵ <http://yahoo.com/>

¹⁶ <http://yahoo.com/>

¹⁷ <http://ware.com/>

URL 1.9	<p>URL Filtering Policy Evaluation Criteria</p> <p>The solution must use the Webroot database only for the categorization and web reputation, all other policy configuration and decisions reside on the VCO / Edge platforms. The “allow”, “drop” or “reject” decision is made based on the following criteria</p>  <pre> graph TD A{URL is in Custom URLs} -- Yes --> B[Process Firewall Policy] A -- No --> C{URL Category ID is available} C -- Yes --> D[Process Firewall Policy] C -- No --> E{Web Reputation is available} E -- Yes --> F[Process Firewall Policy] E -- No --> G[Process Firewall as unknown category] </pre>	HIGH	YAMA ZAKI	
URL 1.10	<p>URL Filtering Policy Actions</p> <p>Based on the criteria listed in the URL 1.7 the Edge platforms takes one of the below actions</p> <ul style="list-style-type: none"> • ALLOW: The HTTP REQUEST forwarded to the Website; no further action taken • DROP: The HTTP REQUEST is silently dropped no further action taken • REJECT: The HTTP REQUEST dropped, and a REJECT message page is sent as a response to the user.  <p>LOG action can be enabled for each of the above options. If configured, the URL Filtering log message must be generated (please see LR 2.7 for more details)</p>	HIGH	YAMA ZAKI	

URL 1.11	URL Filtering Policy Actions with DNS Based on the criteria listed in URL 1.6 and URL 1.7 the edge platform must provide option to enforce URL filtering at the DNS level.	MEDIUM	YAMA ZAKI+		
URL 1.12	Customizable Reject Message An Enterprise level configuration option must be provided such that admin can customize the REJECT message sent to user when a URL is blocked due to the URL filtering policy decision.	HIGH	YAMA ZAKI		
URL 1.13	Redirect Option for Reject Message A configuration option must be provided such that admin can choose to redirect the HTTP REQUEST to the corporate internet policy page instead of sending the Reject message when the URL Filtering policy action is Reject	MEDIUM	YAMA ZAKI		
URL 1.14	Override Action for the Reject URLs Along with the Allow, Drop and Reject, a new action called "OVERRIDE" may be provided. The "OVERRIDE" option will allow the user to access the Rejected page with an access key. When a user requests a particular URL / URL category for which OVERRIDE action configured. User will receive a Reject page, with an option to enter the access key. When the right access key is entered, the user will be able to access the blocked website	LOW	YAMA ZAKI		
URL 1.15	Unknown Category Apart from pre-defined categories (1:1 mapping with Webroot Categories), there should be an "unknown" category to catch all URLs where Webroot categorization database does not categorize URLs and no web reputation found for it. An URL is classified into an unknown category when it is not categorized and also not found in the "Custom URL List".	HIGH	YAMA ZAKI		
URL 1.16	SafeSearch Support Safe Search is a feature of Google Search that acts as an automated filter of pornography and potentially offensive content. Option must be provided to Enable Google Safe Search. When the Enforce Google Safe	MEDIUM	YAMA ZAKI		

	Search option is enabled, DNS responses for Google domains should be rewritten to the Google SafeSearch Virtual IP address. And then the clients will always be forced to use forcesafesearch.google.com ¹⁸ for google search.				
URL 1.17	URL DB lookup from edges use IPv4 and use IPv6 if supported by the DB & where applicable.	MEDIUM	YAMAZAKI		
URL 1.18	Provide users ability to configure URL Filtering by Category and by Reputation as object groups (as highlighted in URL 1.5). Refer to slides ¹⁹ for details.	HIGH	YAMAZAKI		
URL 1.19	Allow users to choose any one of the of user defined URL Category and/or URL Reputation object group(s) as part of Firewall rule creation. Refer to slides ²⁰ for details.	HIGH	YAMAZAKI		
	Security Groups				
SG 1.1	<p>Security services like IDS/IPS, URLF, Malicious IP are created as configurable objects. Security Groups is an object that provides users ability to group all security services objects. Security Group objects can be used in a firewall rule configuration for easy service configurations. Users must be provided with an option to choose between selecting a Security Group vs. individual named security service object selections. The named security service objects based selections in the firewall rule can be implemented for future release. Security services group based selections in firewall rules is required for Yamazaki.</p> 	HIGH	YAMAZAKI		

¹⁸ <https://forcesafesearch.google.com>

¹⁹ <https://onevmw.sharepoint.com/p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

²⁰ <https://onevmw.sharepoint.com/p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

SG 1.2	Security Group object can be used in a firewall rule as shown in slides ²¹ .	HIGH	YAMA ZAKI		
--------	---	-------------	----------------------	--	--

²¹ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

12 6.4 Management Plan Requirements

12.1 6.4.2 URL Filtering

#	Requirements	Import ance	ETA	Jira Issue	Engin eering Respo nses
	URL Filtering				Velo
MP 1.1	<p>URL Filtering configuration must integrate with the existing firewall configuration using named service object creation. URL Filtering capabilities (Category and Reputation based matches) are exposed as named feature objects which are made available as selections in Security services group creation process. Refer to slides²² for details.</p> <p>URL Filtering engine is enabled when Enhanced Firewall services is enabled either at Profile or at Edge level. The service is integrated into the Firewall rule creation flow as one of the security object group selection.</p> <p>Refer to slides²³ for details on feature object creation, integration into security group creation and firewall rules.</p>	HIGH	YAM AZA KI		
MP 1.2	The “Any” option for the URL filtering allows all URLs without any restriction, and this option is as good as URL Filtering is disabled.	HIGH	YAM AZA KI		
MP 1.3	<p>A new “Object Group” section is created under Security and must allow selecting the URL Group name.</p> <p>URL Group are created and defined in the Security Object Group Section (please see REQ URL1.1). Refer to slides²⁴ for details.</p>	HIGH	YAM AZA KI		

²² <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

²³ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

²⁴ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

#	Requirements	Importance	ETA	Jira Issue	Engineering Responses
MP 1.4	“Define” option lists the URL categories and allows select a specific URL category. Also, provide a search bar on the top to search the specific URL category. The URL categories defined are independent of the application definitions provided through Appmap.	HIGH	YAMAZAKI		
	IDS/IPS, Reputation & Threat Intelligence				
MP 1.5	IDS/IPS selection must integrate with the existing firewall configuration. IDS/IPS configurations are exposed as new named feature objects which are made available as selections in Security services group creation process. Refer to slides ²⁵ for details. IDS/IPS engine is enabled when Enhanced Firewall services is enabled either at Profile or at Edge level. The service is integrated into the Firewall rule creation flow as one of the security object group selection. Refer to slides ²⁶ for details on feature object creation, integration into security group creation and firewall rules.	HIGH	WOODFORD		
MP 1.5.1	Provide users ability to create IDS/IPS configurations as object groups. Refer IPS 1.11 and to slides ²⁷ for details.				

²⁵ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

²⁶ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

²⁷ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

#	Requirements	Importance	ETA	Jira Issue	Engineering Responses
MP 1.6	<p>IDS/IPS and Reputation (exposed as Malicious IP Filtering support) selection must integrate with the existing firewall configuration.</p> <p>Malicious IP Filtering configurations are exposed as new named feature objects which are made available as selections in Security services group creation process. Refer to slides²⁸ for details.</p> <p>Malicious IP Filtering engine is enabled when Enhanced Firewall services is enabled either at Profile or at Edge level. The service is integrated into the Firewall rule creation flow as one of the security object group selection.</p> <p>Refer to slides²⁹ for details on feature object creation, integration into security group creation and firewall rules.</p>	HIGH	YAMAZAKI		
MP 1.6.1	<p>Malicious IP Filtering</p> <p>IP reputation score provides the trustworthiness of IP. Most popular solutions (like Webroot) track the IP's overtime for the malicious and inappropriate content and assign a score between 0 to 100.</p> <ul style="list-style-type: none"> • 81-100: Trustworthy • 61-80: Low risk • 41-60: Moderate risk • 21-40: Suspicious • 01-20: High risk <p>VMware solution must provide ability to use reputation scores as part of Malicious Ip Filtering enforcement. Selection of score categories and their inclusions must be made available as configurable settings at the profile/edge level. Rules enabling Malicious IP (as highlighted in MP 1.6) will further be subjected to using the reputation score based settings in allow/block of traffic.</p>	HIGH	YAMAZAKI		

²⁸ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

²⁹ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

#	Requirements	Importance	ETA	Jira Issue	Engineering Responses
MP 1.6.2	Provide users ability to create Malicious IP configurations as object groups. Refer IPS 1.14 and to slides ³⁰ for details.	HIGH	YAMAZAKI		
MP 1.6.3	Provide users ability to create a security group as object group to group security service objects. Refer SG 1.1 and to slides ³¹ for details.				
MP 1.7	Provide ability to view the signatures installed on edges.	HIGH	XANTE	VLENG-117794 ³²	
MP 1.8	Provide ability to manually upload signatures	HIGH	YAMAZAKI+	VLENG-125457 ³³	
MP 1.9	Provide ability to choose signature bundles to use on a profile / edge. Similar to NSX Manager, users are able to choose between default and last 2 versions of the signature bundles.	HIGH	YAMAZAKI+	VLENG-125457 ³⁴	
MP 1.10	Provide ability to view status of signature updates on edges. Signature status is indicated by success and upon looking at details, the list of signature events on the edge can be presented.	HIGH	YAMAZAKI+	VLENG-125457 ³⁵	
MP 1.11	Provide ability to do Signature Management - Ability to modify/customize signatures, exclude signatures	HIGH	YAMAZAKI+	VLENG-125457 ³⁶	
	Reports				

30 <https://onevmw.sharepoint.com/p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

31 <https://onevmw.sharepoint.com/p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

32 <https://jira.eng.vmware.com/browse/VLENG-117794>

33 <https://jira.eng.vmware.com/browse/VLENG-125457>

34 <https://jira.eng.vmware.com/browse/VLENG-125457>

35 <https://jira.eng.vmware.com/browse/VLENG-125457>

36 <https://jira.eng.vmware.com/browse/VLENG-125457>

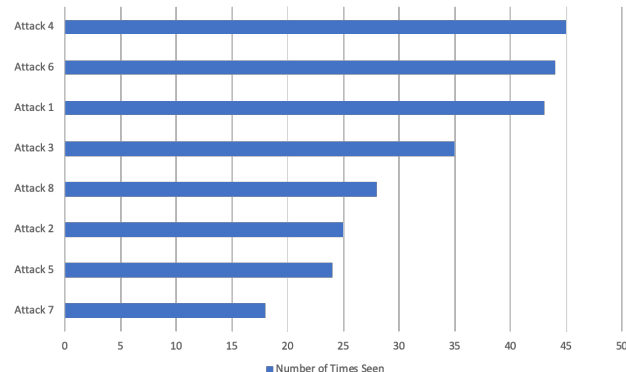
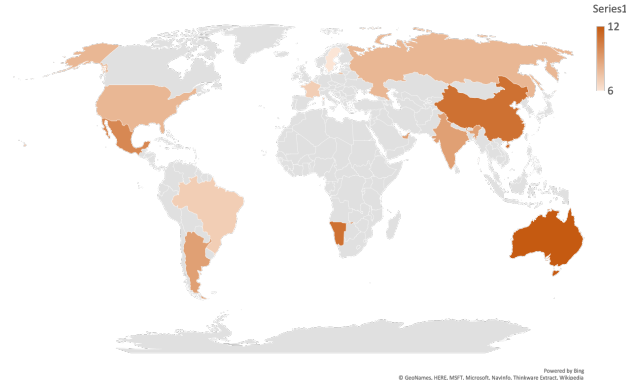
#	Requirements	Importance	ETA	Jira Issue	Engineering Responses
MP 1.1 2	Add following IDS/IPS metrics to SD-WAN standard reports (Quick and Custom) <ol style="list-style-type: none"> 1. Top Threats Detected (By Count, By Impact) 2. Top Threat Origins (By Country, By IP Addresses) 3. Top Impacted Clients (By IP Addressses) 	HIGH	YAMAZAKI	VLENG-122583 ³⁷	
MP 1.1 3	Add following URL Filtering and Reputation metrics to SD-WAN standard reports (Quick and Custom) <ol style="list-style-type: none"> 1. Top Websites 2. Top Web Categories 3. Top Web Reputations 4. Top IPs Blocked (Reputation) 	HIGH	YAMAZAKI	VLENG-122583 ³⁸	

³⁷ <https://jira.eng.vmware.com/browse/VLENG-122583>

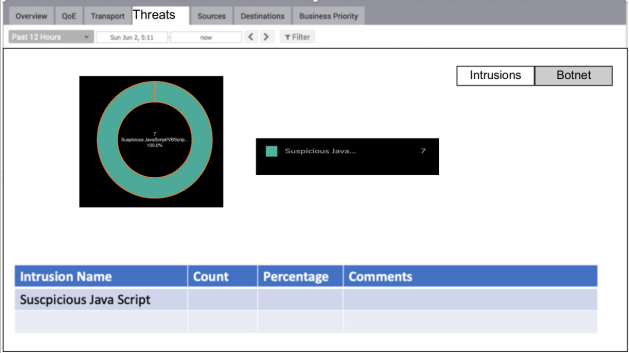
³⁸ <https://jira.eng.vmware.com/browse/VLENG-122583>

13 7.0 Logging, Reporting, Alarm, and Troubleshooting

#	Requirements	Importance	ETA	Jira Issue	Engineering Responses
	Monitoring				Velo
LR 1.1	The customer should be able to monitor Threats & Traffic for the edge in the Monitor Dashboard. Monitoring dashboard supports a customer configurable timeline (Past 60minutes, Past 8 hours, Past 12 hours, Past 24 hours, Past 7 days, Past 2 weeks, Past 30 days) for display of data.	HIGH	WOOD FORD		

#	Requirements	Importa nce	ETA	Jira Issu e	Engine ring Respon ses																		
LR 1.2	<p>MVP Widgets for Threats under Monitor dashboard must include data for - Top Threats by type (intrusions, botnets, virus, spyware as supported by NSX ATP) and Threats by Geo distribution.</p> <div><p>Top IPS Attacks</p><table border="1"><thead><tr><th>Attack</th><th>Number of Times Seen</th></tr></thead><tbody><tr><td>Attack 4</td><td>45</td></tr><tr><td>Attack 6</td><td>44</td></tr><tr><td>Attack 1</td><td>43</td></tr><tr><td>Attack 3</td><td>35</td></tr><tr><td>Attack 8</td><td>28</td></tr><tr><td>Attack 2</td><td>25</td></tr><tr><td>Attack 5</td><td>24</td></tr><tr><td>Attack 7</td><td>18</td></tr></tbody></table><p>Threat Map</p><p>Series1 12 6</p><p>Powered by Bing © GeoNames, HDRE, MSFT, Microsoft, NavInfo, Thinkware Connect, Wikipedia</p></div>	Attack	Number of Times Seen	Attack 4	45	Attack 6	44	Attack 1	43	Attack 3	35	Attack 8	28	Attack 2	25	Attack 5	24	Attack 7	18	HIGH	WOOD FORD		
Attack	Number of Times Seen																						
Attack 4	45																						
Attack 6	44																						
Attack 1	43																						
Attack 3	35																						
Attack 8	28																						
Attack 2	25																						
Attack 5	24																						
Attack 7	18																						
LR 1.3	<p>Traffic and threats information from the dashboard must allow deeper investigation and provide ability to correlate to the logs context.</p>	MEDIU M	WOOD FORD																				

#	Requirements	Importance	ETA	Jira Issue	Engineering Responses
LR 1.4	<p>URL Reporting in VCO</p> <p>When we support log collection and aggregation of URL ALLOW and DROP / REJECT messages, the VCO must support graphical reporting of ALLOWED and DROP / REJECT URL</p> <p>Under Security Overview, a new tab called “Web” must be created in Edge → Monitoring page to display top Web sites blocked.</p> <p>A Table at the bottom with decreasing order of top URLs. A table will have the following columns</p> <ul style="list-style-type: none"> • URLs • Categories • URL Reputation • Total Hits 	HIGH	YAMA ZAKI		

#	Requirements	Importance	ETA	Jira Issue	Engineering Responses
LR 1.5	<p>Threats Reporting in VCO</p> <p>VCO must support graphical reporting of Threats for Intrusions and Botnet (Reputation). Similar to the Application monitoring tab, a new tab called “Threats” must be created in Edge → Monitoring page, please see mockup below</p>  <p>Intrusions / Botnet buttons – A toggle button, changes the display information relates to Intrusions vs. Reputation based blocking.</p> <p>A Table at the bottom with decreasing order of top Intrusions/Blocked IP. A table will have the following columns</p> <ul style="list-style-type: none"> • Name (Intrusion/Botnet) • Count (No. of hits) • Percentage (% hit for an intrusion/botnet across the total number) • Comments (Additional description about the intrusion/botnet blocked) 	HIGH	WOOD FORD		
	Logging				
LR 2.1	<p>The customer should be able to monitor security & firewall logs on VCO. Support must be provided to store logs locally on VCO. Default log retention for firewall including ATP events should be 2 weeks. Customers will have the option to subscribe to additional retention (up to a year). Details of log</p>	HIGH	WOOD FORD		

#	Requirements	Importance	ETA	Jira Issue	Engineering Responses
	retention and compliance to use same requirements as defined in the Logging Infra PRD ³⁹ .				
LR 2.2	Logging for Blocked traffic for IDS/IPS, Malicious IP Edge must generate a firewall log (Syslog format) message when an intrusion is blocked and logging is enabled. It is recommended to send these log messages to the configured external syslog server/ SIEM. Syslog field extension for security events must include message fields (Intrusion events, Botnet) as defined and supported by the NSX Solution. See link below on logging field used with IDS/IPS from NSX - https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-100D9BB2-CC4A-4AA0-B117-10ED4B113F0D.html https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-852AADD3-653F-4C1C-A10E-24D03B4084CA.html Example IPS log for Fortinet (competitor) - https://docs.fortinet.com/document/fortigate/7.2.0/fortios-log-message-reference/311596/ips-log-support-for-cef	HIGH	WOOD FORD		
LR 2.3	Format of ATP log message ATP logs must include all the fields as supported by the NSX ATP solution	HIGH	WOOD FORD		
LR 2.4	Firewall logs w/ threat info can be sent to an external syslog server specified by the customer	HIGH	WOOD FORD		
LR 2.5	Logging for Drop / Reject URLs The Edge must generate a firewall log (Syslog format) message when a URL is Dropped / Rejected and logging is enabled. It is recommended to send these log messages to the configured external Syslog server / SIEM.	HIGH	YAMA ZAKI		

³⁹ <https://confluence.eng.vmware.com/display/VELOPROD/VCO+Logging+Infrastructure>

#	Requirements	Importance	ETA	Jira Issue	Engineering Responses
LR 2.6	Logging for Allow URLs The Edge must generate a firewall log (Syslog format) message when a URL is allowed and logging is enabled. It is recommended to send these log messages to the configured external Syslog server / SIEM. Collection and aggregation of URL allow messages in VCO is only available for the demo environment.	HIGH	YAMA ZAKI		
LR 2.7	Format of URL Filtering Log Message The format of the URL Filtering log message must comply with the existing firewall log message format. And it must have below additional fields in the log message (addition to the Session-Open / Session-Deny) <ul style="list-style-type: none"> • Log Source = "URL Filtering" • Requested URL • URL Category Example Web Filter log Fortinet (competitor) - https://docs.fortinet.com/document/fortigate/7.2.0/fortios-log-message-reference/400992/webfilter-log-support-for-cef	HIGH	YAMA ZAKI		
	Alarm and Troubleshooting				
LR 3.1	High CPU and Memory Utilization Alerts The system must report high CPU and memory utilization due to the increased load on the IPS engine. The system generates an Alert / Syslog message and sends it to the VCO and configured external log servers VCO must display these alerts and Syslog messages.	HIGH	YAMA ZAKI		

#	Requirements	Importance	ETA	Jira Issue	Engineering Responses
LR 3.2	<p>Behavior Under Load</p> <p>The IPS system must continue to operate under the load. In case the load increase beyond the threshold the IPS system no longer able to process the packets, then the default setting is to Allow.</p> <p>A configuration option must be provided to change this behavior to default Block. This configuration is only available to the Cloud / Tech Ops.</p>	MEDIUM	WOOD FORD		
LR 3.3	<p>Fail Open Mode</p> <p>In the case of IPS module crash or any other system-level failure, the system becomes fail open (allow all traffic)</p>	MEDIUM	WOOD FORD		

14 8.0 Performance and Scale Requirements

Platform	Firewall Throughput w/o ATP (1300-byte)	Firewall Throughput with ATP (1300-byte)	Firewall Throughput w/o ATP (IMIX)	Firewall Throughput with ATP (IMIX)
Edge 510	350 Mbps	250 Mbps	200 Mbps	150 Mbps
Edge 510-LTE	350 Mbps	250 Mbps	200 Mbps	150 Mbps
Edge 520	350 Mbps	250 Mbps	200 Mbps	150 Mbps
Edge 520v	350 Mbps	250 Mbps	200 Mbps	150 Mbps
Edge 540	1 Gbps	700 Mbps	500 Mbps	350 Mbps
Edge 840	4 Gbps	2.8 Gbps	1.5 Gbps	1 Gbps
Edge 3400	7 Gbps	4.9 Gbps	2.5 Gbps	1.7 Gbps
Edge 2000	10 Gbps	7 Gbps	5 Gbps	3.5 Gbps
Edge 3800	10 Gbps	7 Gbps	5 Gbps	3.5 Gbps
Edge 620	1.5 Gbps	1 Gbps	750 Mbps	500 Mbps
Edge 640	3 Gbps	2 Gbps	1 Gbps	700 Mbps
Edge 680	6 Gbps	4 Gbps	2 Gbps	1.5 Gbps

15 9.0 Open Questions

Question	Answer	Date Answered

16 10.0 Out of Scope

17 Edge Firewall ATP Services - SASE SE/SA Feedback

Name	Feedback
Trevor Gerdes	<ul style="list-style-type: none"> • It is important that logging can also go via Syslog from edge to customers SIEM, and that we publish definitions of log categories. • We have lots of push back about having to write custom scripts to pull logs from VCO. • Some sort of live logging of events in the troubleshooting page should to be there as well. • Only needs to be the last 100 or so events for a specific source, destination or rule.
Saqeb Akhter	<ol style="list-style-type: none"> 1. Is there other VCE FW improvements in Woodford other than ATP – I know we have had complaints that our VCE FW is not very easy to use/configure 1. Enhancements to object groups? 2. Integration with logging framework? (or will the SYSLOG FW events be extended?) <ul style="list-style-type: none"> • We’ve also all tried to use the FW to block I7 applications – without first packet match it doesn’t work well , and the traffic gets allowed when it shouldn’t be 1. “deny all” outbound rules don’t work because of this 2. Just this week we have a 5000+ branch opportunity in Brazil where we were not able to reliably block login.live.com⁴⁰ – because of the way we do dns<>ip caching, and sni fqdn blocking -- > when the URL filtering is enhanced for woodford – let’s make sure scenarios like this work. (Customer claimed Fortinet worked)
Juan Regina	On IDS/IPS, will we be able to whitelist specific files (hashes) on day-1?

⁴⁰ <http://login.live.com>

Name	Feedback
Mir Ali	<p>Few observations and feedback that might be helpful in phase 2 moving forward..</p> <p>TLS1.3 encrypts SNI info, even though not lot of sites aren't doing so at this time , still almost half the traffic on google is tls1.3 encrypted. I am wondering the effectiveness of URL filtering if we are not doing ssl decrypt.</p> <p>Keeping thin branch in mind, in line with SASE architecture is to have two categories –</p> <ul style="list-style-type: none"> • Decrypt – traffic that is tls 1.3 encrypted or need full decryption to effectively categorize whether to allow or block, send this traffic to SASE POP for SSL decryption for inspection, we can effectively decide whether to block or allow traffic . Running SSL decryption on edge will cut the performance is half. • No- Decrypt – e.g. financial, banking, gov. or any sites customer choose not to decrypt and/or use basic URL filtering on edge. • This still doesn't stop day 1 aka zero-day threats as edges will pass first few packets until the hash is identified as threat by SASE POP/DB, for zero day we need ML which is completely different project in itself , other vendors like PA use ML, pattern matching , domain analysis, behavior analysis etc to block zero-day threats in cloud and use implicit deny. • Implicit deny capability option on edges will help zero day. i.e., deny everything by default unless specified.
Nick Barrett	<p>Regarding @Saqeb Akhter⁴¹'s requests,</p> <p>I think there are 2 main problems:</p> <ol style="list-style-type: none"> 1. Firewall rules matching destination domains – common with object groups. Done in this fashion, it isn't looking at HTTP Host header or HTTPS SNI value. It uses the domain <-> IP cache which causes lots of false-positive matches. URL filtering is often what people are expecting in this situation. Our UI doesn't really make it clear that this is effectively DNS reverse lookups to enforce the policy. 2. Matching applications that are HTTP(S). <ol style="list-style-type: none"> 1. A massive share of the SD-WAN (QOSMOS) applications is based on HTTP(S) and customers expect the firewall policies to work for them. 2. Other vendors' application control policies will allow the HTTP(S) session to setup so that the SNI or Host fields (or deeper) can be inspected before making a verdict while still maintaining default-deny. 3. This is done by having an intermediate DPI result that their application recognition engine uses to indicate that there are multiple allowed candidates that the session could match eventually. So, the packet is permitted, and DPI continues for the session until a verdict is made and then allowed/dropped/blocked & logged. 4. It seems the way we use QOSMOS today causes those types of intermediate results to spill over to the default firewall policy which many customers want to be a deny-all. QOSMOS never gets a chance to correctly ID the application.

41 <mailto:akhters@vmware.com>

Name	Feedback
Vlad Franca De Sousa	One question I have around IPS/IDS , all slides so far seems to implicate these will only apply to internal traffic or non-web traffic towards “cws” so I am still not clear is if we will be able to use the NGFW to inspect Web Traffic towards Internet as well. Isnt there ids/ips signatures that are looking at Web traffic, and those could be external.

18 Sept. 16 Meeting Notes with Tom Speeter

Notes from the meeting with Tom. Please add/edit anything that I missed:

1. Tiers of firewall logs. Talk to the PM team on the tiers.
 - a. Tier 1 – Logs shown on the UI
 - b. Tier 2 – Months of logs for forensic analysis
 - c. Tier 3 – Entire logs for the customer (from Amazon EBS volumes)
2. Timestamp granularity of the logs – milliseconds should be sufficient as nanoseconds could be overkill. Also, current edges may not process it at nanoseconds level
3. Data retention based on fixed time interval (days/weeks/months) may not be the same for customers who have more edges with high traffic than who have less edges with low traffic. Discuss with PM team as to how to package this in the product
4. Data migration to ClickHouse (based on current data retention)
5. ClickHouse ingestion pipelines should be durable to make sure all logs are inserted
6. *Deny* logs are comparatively small and more manageable than *allow* logs which could vary from Million logs per day vs Million logs every 5 mins depends on the customer
7. Current logs table have partition based on month with sub partition by edge (id mod 8)
8. Processing queue table processes all logs, flow stats etc. Talk to Kaushik team to understand more on the recent changes
9. *Allow* and *Deny* logs should be sold as separate features, as Allow logs are orders of magnitude greater. Even with per-flow rollup.

19 VCE Enhanced Firewall Services - PM/Dev/TME/UX Weekly Sync

19.1 Yamazaki Release Open Issues

Item	Description	Owner	Status	Date	Comments
1.	UX Mockups for Security Objects	@Ritesh Tiwari	COMPLETE		Refer to slides ⁴² for details.
2.	PRD Approval for URLF / IP Reputation	@Preethi Nandakumar @Adam Schultz @Unknown User (saravanan k)	COMPLETE		Post security group design, PRD updated and dev teams to provide re-approval of the PRD.
3.	PRD Approval for support of FW/ EFS for Inbound ACL settings	@Adam Schultz @Unknown User (saravanan k) @Aditya Agarwal	IN PROGRESS		Edge Firewall & EFS w/ Inbound ACL Settings (1:1 NAT & Port Forwarding) ⁴³ - PRD

⁴² <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/FW%20Security%20Groups.pptx?d=w27afba9729514c319f83f3c1a1e73d2a&csf=1&web=1&e=TYkBvA>

⁴³ <https://vmw-confluence.broadcom.net/pages/viewpage.action?pageId=1757503990>

Item	Description	Owner	Status	Date	Comments
4.	PRD Approval of FW Log Actions	@Aditya Agarwal @Ritesh Tiwari	IN PROGRESS		Refer to slides ⁴⁴ for details.
5.	Firewall Enhancements requests for Yamazaki	@Preethi Nandakumar	IN PROGRESS		
6.	DP / MP QE Test Plan Approval	@Abhijeet Bhoyar @Avinash Bhoomiredy	COMPLETE		
7.	UX mock up for Monitoring dashboard	@Ritesh Tiwari	COMPLETE		10/31: UI for Enterprise view is ongoing, Edge view requirements are done
8.	UX mock up for Logging (fields required for each of the engines, default display)	@Ritesh Tiwari	COMPLETE		
9.	Performance improvements for EFS (based on SD-WAN optimization improvements in Xante)	@Unknown User (saravanan k)	IN PROGRESS		Investigation started. Performance numbers are retested by the QE team for EFS based on appropriate flow limits.

⁴⁴ <https://onevmw.sharepoint.com/:p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/Edge%20FW%20Log%20Actions.pptx?d=w41b3937d269240969977bac74f4e1ed5&csf=1&web=1&e=HMAZhr>

Item	Description	Owner	Status	Date	Comments
10.	Document System behavior when individual features are turned on/off (UI/documentation); Ex: if IDS/IPS is turned off, does this translate to increased max flows? What happens to existing flows?	@Gobu Ezhumalai @Ramprasath G R @Praveen Kumar Rajendran	COMPLETE		<p>5.2 - Suricata initialized and flows reduced by half;</p> <p>6.0 - Flows reduced by half only when IDS/IPS is enabled; Not for URLF/ Reputation engines</p> <p>@Praveen Kumar Rajendran check on the pop up behavior for turning on/off URLF, Reputation and IDS/IPS.</p> <p>10/31: @Ramprasath G R tabulate DP behavior for various feature level knob changes</p>
11.	Security Feature / Group Naming	@Sathya Thammanur	COMPLETE		<p>PMM has proposed to use "Enforcement" instead of Security features. Work in progress to finalize naming.</p> <p>10/25: Lock the naming changes in a week</p> <p>Security Services, Security Service Groups - Naming locked for 6.0 release</p>
12.	Security Engine behavior when Firewall log is not enabled	@Unknown User (saravanan k) @Aditya Agarwal	COMPLETE		<ul style="list-style-type: none"> Denies are always logged Allow and log's will be captured if log is enabled for a given security engine (even if firewall log is not enabled)
13.	Provide text for unclassified web traffic	@Sathya Thammanur	COMPLETE		<p>10/25: Provided text to @Ritesh Tiwari</p>

Item	Description	Owner	Status	Date	Comments
14.	Provide default logging fields	@Sathya Thammanur	COMPLETE		10/25: Defaults provided to @Ritesh Tiwari
15.	QE Test plan - Ensure that complete URL categorization is tested (not just domain) for HTTP traffic	@Abhijeet Bhoyar	IN PROGRESS		
16.	Logging mechanism - Individual engine log vs. aggregated log per flow	@Gobu Ezhumalai @Aditya Agarwal @Ramprath G R	COMPLETE		10/25: Decision: Individual logs generated for IDPS, IP Filtering and URLF engines. Open item: URLF (category & reputation) log aggregated or split up pending. 10/31: IDPS, IP Filtering and URLF Engines will generate individual logs; URLF will aggregate logs for reputation and category based filtering
17.	File a JIRA for URL Filtering behavior	@Ramprath G R	IN PROGRESS		10/31: Integration testing revealed issue with URL's not getting enforced for second URL lookup.
18.					

19.1.1 Yamazaki FW Feature Target List & Status⁴⁵ - List of features targeted for Yamazaki including status for PRD, UX, FS approvals.

19.2 Woodford Release Open Issues

Item	Description	Owner	Status	Date	Comments
1.	Confirm models supported with ATP	@Preethi Nandakumar	DONE		Need confirmation on support for 5xx series, 6xx series and above; 510/520 potential issues with memory
2.	Severity scoring computation with IDS/IPS	@Ramprasad G R	DONE		<p>Need closure on severity level computation used; Plan to mimic NSX Manager methodology for severity and impact score reporting</p> <p>5/10: Dustin, Derek, Sathya met with Raju/Rajitha from NSX. NSX uses only signature_severity field from the JSON file. Dustin to write up the severity mapping and share with the team to implement for Woodford</p>

⁴⁵<https://onevmw.sharepoint.com/p:/r/teams/velo-products/Shared%20Documents/SASE%20Security/edge-firewall/Yamazaki-Edge-FW-Feature-Status%20Sep%202023.pptx?d=wd37166d465d7413e8abeb108f2563ab6&csf=1&web=1&e=Tjivvl>

Item	Description	Owner	Status	Date	Comments
3.	Licensing SKU support	@Aditya Agarwal	DONE		Licensing SKUs are now available; Customer capability for EFS will be enabled by Maestro ; Provide build for Maestro team to test license/ customer capability enablement - Post Woodford activity 6/7: Per @Ramya Narayana licensing support is enabled for EFS add-on SKU.
4.	CPS drop closure	@Gobu Ezhumalai	DONE		Closure on CPS drop with ATP enabled; File extraction on SMTP disabled
5.	ATP On-Prem Deployment Model	@Sathya Thammanur	DONE		Need an on-prem deployment model worked out with COE team; Create process similar to SASE security SASE on-prem Deployment - VMware SASE Cloud with Partner on-prem VCO ⁴⁶ Email: sase-coe-all alias for on-prem vco support/ enablement
6.	ATP Naming Finalized	@Unknown User (aakhter)	DONE		Naming of ATP changed to Enhanced Firewall Services. Naming change has been implemented in UI and documentation.

⁴⁶ <https://vmw-confluence.broadcom.net/display/VPDT/SASE+on-prem+Deployment+++VMware+SASE+Cloud+with+Partner+on-prem+VCO>

Item	Description	Owner	Status	Date	Comments
7.	New customer ATP Add-on Fulfillment model	@Sathya Thammanur	NOT APPLICABLE		Gartner deadline for ATP requires SKU is available and deployable on GA. Need to work a model with Edge ops for VCO upgrade/ support for 5.2 release on GA date.
8.	Finalize ATP Add-on Pricing	@Sathya Thammanur @Eric Kong	DONE		Approval complete on 4/17
9.	ATP Pendo support / workflow	@Sathya Thammanur	DONE		Working with Vardit to create Pendo Workflow for 5.2 release
10.	Partner super user not able to enable EFS	@William Zapata @Sathya Thammanur	DONE		@Sathya Thammanur Sync w/ Sandeep/Kishan to figure behavior for Customizable QoE. 6/6: @William Zapata to address support in 5.2.1 release; Preethi to confirm testing possible in 5.2.1 release. Fixed in 5.2.1 release.
11.	Enable Firewall Logging to VCO Workflow - enabled by Maestro	@Sathya Thammanur	DONE		@Sathya Thammanur Work with Ramya for Maestro to enable Firewall logging to VCO along with EFS as part of EFS order fulfillment. 6/7: Per @Ramya Narayana Logging support is enabled for EFS add-on SKU.

Item	Description	Owner	Status	Date	Comments
1 2.	Close out Datasheet updates for EFS	@Sathya Thammanu r	DONE		6/7: Provided datasheet performance metrics to Vivian for publish.

19.3 PRD Review Meetings

Meeting Date	Meeting Minutes
9/22/ 22	Logging/Monitoring & Management Plane Review https://VMware.zoom.us/rec/share/c6svbN5scUDSK09jAvkCzdWKNarHEcRd4zj83mM7ISY3QfxbRWnVbFcg-VlhdPXa.mJxuvUp0aaz8G_XS Passcode: 8f9A5N.p
10/4/ 22	Data Plane Review https://VMware.zoom.us/rec/share/j_Hv9lX1gZe4rk7IOL40k2CJdlI0aKuEIlmqIrdQmAGt5BCZPRFq7cma_1W-kBfR.1yjiZNgTuAzADbjB Passcode: s7q1z52!
10/6/ 22	Firewall Policy Enhancements https://VMware.zoom.us/rec/share/Lzxgli8t7w6rdO-8ITJZ8h6dOlxAblNFLQ1aJjBryhgzg6taDqF9MRt2sFaOCqOBA.teobbSj4iybl78ID ⁴⁷ Passcode: VC?Tq8h5
10/26 /22	FedRamp Requirements https://VMware.zoom.us/rec/share/vXuUfJADagtB1mOibnd-xp11xEtqlUPxrK9uLMZQ81Rh4F1ztQiXAXxng3wYgLM.mF1P4DNMQcME39sS ⁴⁸ Passcode: hr2?7s&N

⁴⁷ <https://vmware.zoom.us/rec/share/Lzxgli8t7w6rdO-8ITJZ8h6dOlxAblNFLQ1aJjBryhgzg6taDqF9MRt2sFaOCqOBA.teobbSj4iybl78ID>

⁴⁸ <https://vmware.zoom.us/rec/share/vXuUfJADagtB1mOibnd-xp11xEtqlUPxrK9uLMZQ81Rh4F1ztQiXAXxng3wYgLM.mF1P4DNMQcME39sS>

Meeting Date	Meeting Minutes
10/31/22	Edge Firewall Logging Requirements / Cost Modeling https://VMware.zoom.us/rec/share/Y8Qua5LHx8LShjO7tLBpB1pIAyJTqISH8LrfGnP7lvp9JWMSdUjZ0j1fWSwxUemK.ZwTfjqwaj1HI6q5Q ⁴⁹ Passcode: 3&r@=rB+
3/23/23	URL Filtering / Reputation (Part 1) https://VMware.zoom.us/rec/share/fJu4RRlvcTaU7Q8wVpZg6lpChrHjMu7tXT6WE9fMSuOKD_Au86kM9PJcF8DCgBBB.3vTvMmwUEZnEmBsN Passcode: y7C2t*7F
3/27/23	URL Filtering / Reputation (Part 2) https://VMware.zoom.us/rec/share/eHdd3R1ilZVD6x5aAHi58lrTuMqaTlyt40GHZZgt3OQaOUH2b-JrgKQRz2kjGgss.S2mtkvdu9ZH5TsaQ Passcode: 9?.4A9DU
3/30/23	URL Filtering / Reputation (Part 3) https://VMware.zoom.us/rec/share/meTsLL9VunhhBCguLV4GVWrrDH1wSo-dhX4tz8rdJEngjHVxVh9MSLx8EJBmee5S.-6fSEMM-gp3ZehZ Passcode: 3+YP4f0U
3/31/23	URL Filtering / Reputation (Part 4) - Approval Session https://VMware.zoom.us/rec/share/zhGh9Boa6mbfdyvOCPhl8Kq7kD6tncpS_zKoTqV8ZNh5fN6U8SL7lgsbdllH4bmY.G3T16by1nv0LRSWa Passcode: jRT4Jy?#
1/23/2024	Security Reporting - PRD Review Session https://broadcom.zoom.us/rec/share/usxUIQexigByXWNPtY_jRrZ05CHu40-WAYqXfBSMIXXdVCSnjj9JEQLPmngRGx_z.erTAQlawG1kGuvDn?startTime=1706026670000 Passcode: j!WPE04@

⁴⁹ <https://vmware.zoom.us/rec/share/Y8Qua5LHx8LShjO7tLBpB1pIAyJTqISH8LrfGnP7lvp9JWMSdUjZ0j1fWSwxUemK.ZwTfjqwaj1HI6q5Q>

Meeting Date	Meeting Minutes
3/5/2024	Security Reporting - PRD Review Session2 https://broadcom.zoom.us/rec/share/xfajetCMkjinRcF2no6tzw_qz3-YPZh3kogj4LsGGGnYVezDDkS8FIBQKQoj5lpzV.fY1rz6dYy7aFYy3u ⁵⁰ Passcode: h5V=h33H
3/12/2024	Security Reporting - PRD Review Session 3 (Q & A / Comments addressed) https://broadcom.zoom.us/rec/share/lvcbvSU4n61KA2yiBLM9mgrBfVqDePS7zU3e_nLDhwwgbPVKEIWUqy77k2Oh8NNu.k5AAcXaX9f1DJp_n ⁵¹ Passcode: M%7Az5n%

19.4 Weekly Engineering/Product Sync Meetings (Internal)

Meeting Date	Meeting Minutes
9/15/22	Attendees - @Thiaga Sankaran @Sathya Thammanur @Unknown User (tprabhu) @Unknown User (qxinzhou) @Unknown User (sankitkumar) @Unknown User (gkasinathan) @Derek Tay @Gurudutt Maiya Belur @Qing Li @Sivabalan Pandian @Aditya Agarwal https://VMware.zoom.us/rec/share/B0_Xkyi6jsXTjNOX9a1gjbOtX-ko_BHtc6voYEo3K-xaz79Jkh-n1w6_N0XOE4.JEReBAHDJdrxR2Qb ⁵² Passcode: #2Kf?4Hv

⁵⁰ https://www.google.com/url?q=https://broadcom.zoom.us/rec/share/xfajetCMkjinRcF2no6tzw_qz3-YPZh3kogj4LsGGGnYVezDDkS8FIBQKQoj5lpzV.fY1rz6dYy7aFYy3u&source=gmail-imap&ust=1710265492000000&usg=AOvVaw0YpX7ttiTgIKvRoukwNr-6

⁵¹ https://www.google.com/url?q=https://broadcom.zoom.us/rec/share/lvcbvSU4n61KA2yiBLM9mgrBfVqDePS7zU3e_nLDhwwgbPVKEIWUqy77k2Oh8NNu.k5AAcXaX9f1DJp_n&source=gmail-imap&ust=1710863299000000&usg=AOvVaw0o8V4iDyq2Tfwi3GEaoYEv

⁵² https://vmware.zoom.us/rec/share/B0_Xkyi6jsXTjNOX9a1gjbOtX-ko_BHtc6voYEo3K-xaz79Jkh-n1w6_N0XOE4.JEReBAHDJdrxR2Qb

Meeting Date	Meeting Minutes
9/22/22	<p>Attendees - @Thiaga Sankaran @Sathya Thammanur @Unknown User (tprabhu) @Unknown User (qxinzhou) @Unknown User (sankitkumar) @Unknown User (gkasinathan) @Derek Tay @Gurudutt Maiya Belur @Qing Li @Sivabalan Pandian @Aditya Agarwal</p> <p>https://VMware.zoom.us/rec/share/zf1w55zF7bdIWROjQAArskuPKrvLkrqD8ZZpkA-zbvDzYPAobyvsbc3TRWg4RRr0.pFXe0xchd-o3pHJH⁵³</p> <p>Passcode: x*7YA5&Y</p>
10/6/22	<p>https://VMware.zoom.us/rec/share/c6svbN5scUDSK09jAvkCzdWKNarHEcRd4zj83mM7ISY3QfxbRWnVbFcg-VlhdPXa.mJxuvUp0aaz8G_XS⁵⁴</p> <p>Passcode: 8f9A5N.p</p>
10/20/22	<p>https://VMware.zoom.us/rec/share/dDAaZFF2CaCmld1vtYuEgxQoGZ18lyzFNN9rcEAWsDUZ421r3SsXtcKfaf5AMKHh.hmPj5UgWpTOnx2ue⁵⁵</p> <p>Passcode: 5eR#1SQ*</p>
11/03/22	<p>https://VMware.zoom.us/rec/share/gclaJknubNXFptULUDpEdwT3NMY3M9iPZ18gL0AAI9bkRNdOVpa0xjuGQuzkoAFg.PvwewXOuABbakWpy⁵⁶</p> <p>Passcode: f4%.s7va</p>
11/10/22	<p>https://VMware.zoom.us/rec/share/WMQgeT7riPyUoRIWBE2vCub58L1gCHWRdv4qrHKXaYIUJT269s0CUG7GxbEg6be.IvtjZE55ZaXe8OV⁵⁷</p> <p>Passcode: fX0E.65=</p>
11/17/22	<p>https://VMware.zoom.us/rec/share/c01IQIDaJ4QyJnB2anPvVD68KZW6x6S5VFu_0NwN2iciz7eHoi0oiG4z2wRxrg_.CTAhWGJBPyVuKeSI⁵⁸</p> <p>Passcode: f\$!eWCc9</p>

⁵³ <https://vmware.zoom.us/rec/share/zf1w55zF7bdIWROjQAArskuPKrvLkrqD8ZZpkA-zbvDzYPAobyvsbc3TRWg4RRr0.pFXe0xchd-o3pHJH>

⁵⁴ https://vmware.zoom.us/rec/share/c6svbN5scUDSK09jAvkCzdWKNarHEcRd4zj83mM7ISY3QfxbRWnVbFcg-VlhdPXa.mJxuvUp0aaz8G_XS

⁵⁵ <https://vmware.zoom.us/rec/share/dDAaZFF2CaCmld1vtYuEgxQoGZ18lyzFNN9rcEAWsDUZ421r3SsXtcKfaf5AMKHh.hmPj5UgWpTOnx2ue>

⁵⁶ <https://vmware.zoom.us/rec/share/gclaJknubNXFptULUDpEdwT3NMY3M9iPZ18gL0AAI9bkRNdOVpa0xjuGQuzkoAFg.PvwewXOuABbakWpy>

⁵⁷ <https://vmware.zoom.us/rec/share/WMQgeT7riPyUoRIWBE2vCub58L1gCHWRdv4qrHKXaYIUJT269s0CUG7GxbEg6be.IvtjZE55ZaXe8OV>

⁵⁸ https://vmware.zoom.us/rec/share/c01IQIDaJ4QyJnB2anPvVD68KZW6x6S5VFu_0NwN2iciz7eHoi0oiG4z2wRxrg_.CTAhWGJBPyVuKeSI

Meeting Date	Meeting Minutes
5/9/2023	https://VMware.zoom.us/rec/share/Aph5IfklNzunkpFvmiXSzoc3cdnAKmhGEE01a-QtKS8eZDOoOOQJ9u2Vk21PEzon.XtjvuJKBRyTze0U9 Passcode: 9c8C%FiZ
5/16/2023	https://VMware.zoom.us/rec/share/projR0gOtpUtBm0tnswpN3GqcnnGoJZ7YpMKKsnte1z0XJ2VCASBFVbQVQBz7H.lkDBtpGanJuzbN0e Passcode: 7pA*Zgp3
6/6/2023	https://VMware.zoom.us/rec/share/3ezMJVsZLHsZhe5xgdbBkHb-CQ58p_QxMs7A0KTu9nDriWVXcyHJoiCI5wnYYUHu.l76B-v20-pkNpqwX Passcode: ju6A&qUs
6/13/2023	https://VMware.zoom.us/rec/share/l-BJcb_IgNORoC4gOyi6s2qqUoBtqgZTUCJrq-00R1yw_moTelYpTC_XskEB3ifd.kpu43eF_dZY_LhtR Passcode: .5cZ5S2u
6/20/23	URL Filtering / IP Reputation POC Review https://VMware.zoom.us/rec/share/egJzgtc0WyhjObmeOx-BAVwDfAQFfuFnQ601jMzwlpHpKtztLWZb2pCPJBtuiWc.pCO-ih0qaYWFzAxI Passcode: 6BN.aX&d
7/25/2023	https://VMware.zoom.us/rec/share/dx3PPq0rsxsqk8gCoRzRMp93MYqoDICHalbgL25gyAghJAcQv5NIKUtviaH0ulrP.U61GvolpkLsLGusw Passcode: 1&Y7A%j#
8/1/2023	https://VMware.zoom.us/rec/share/CL47V971axMV-1Y37EEoEWVEYMgG1YJKMZK_1YGUQqyLusHqER7o3_Lyq-38Qpr5.RLLWuqVLTE8beN5L Passcode: 3wB#X09S
8/9/2023	https://VMware.zoom.us/rec/share/osV78lqmM2XFj0XxWXJPtxzrJiw9MXLXMqCljwhNwcGsuVUXNCx4WsMCMickHqz4.nYn2LL1LuiKqsWph Passcode: BZb6\$U9?
8/15/2023	https://VMware.zoom.us/rec/share/Gf7Kls-vRqLS4v1q_EVai21tckYYYYF-tNkUuwcJsmuk1IU71LgYi7LE511NtX4B2.10QC1COseSp_Uby3 Passcode: V^3W@yw1

Meeting Date	Meeting Minutes
8/22/2023	https://VMware.zoom.us/rec/share/6YWrD6Y3O-lsnKjoMB0kMC6qatWv_HR1w8vwGGTPFUEBB9dSUR-dU_j-qXFLKpkL.FROI8-lrEj6thcN9 Passcode: U&9K=@Dg
8/29/2023	https://VMware.zoom.us/rec/share/ru1uwtIXdFgS65fYQHTQDoQeA3_MZv15c-cgPGkCGoMo3xs5c8cTyWaeXawla_u0.5ZwE9B83KUI5mj1d Passcode: *67i%0*M
9/19/2023	https://VMware.zoom.us/rec/share/cnkZxMYLjn8OCT8JDBYC7ulbND2XI-IAAttgPW6nv3CZG-a-kHtMMylVWKQT-O_t.gbDdEymO8_1povEA Passcode: +BDSU4R9
9/26/2023	https://VMware.zoom.us/rec/share/Afi91N_wVbsoZlBaLFvj4kNXmPIENZtieVSbu9F9T-xmsx3WSvmk2J3vmz3bDS3G.ztzuBXdtJJ0Cdgl Passcode: rd5w+5pM
10/3/2023	https://VMware.zoom.us/rec/share/NbXreNxc4jRrld83mLt9WQBIK2m1Fe89FGRvkiEaR0yP04FcYxfHFR7kah5RznCb.n5A5TRoJpetlV7as Passcode: 1uj!rjGR
10/17/2023	https://VMware.zoom.us/rec/share/GTYLNwT-2mcJHen_rsDoVH0Xk6gkdfkDWBgfWI_jFKCiKS2xDXhNBnvaja3AjHbv.BWX2uoVcdJ_pU0Fs Passcode: ==4MzNJo
10/25/2023	https://VMware.zoom.us/rec/share/RGmg07VI88c6CnbbFr_G4-7tW-ZqEOXR0zPddJ_OyQVWjPZ-zCEzVAK66ZzqHaQW.73isxPoU2lwl6-4o Passcode: !aZKx^u8
10/31/2023	https://VMware.zoom.us/rec/share/DSnFR7fNYM3R8kfa6Dng1Yk76NKpkE3D6oi_WU16aS2LOaCy9IHxFxPbv7566Jag.8wWxw_6TVI oBYkoh Passcode: Pa%d^#%0

Meeting Date	Meeting Minutes
11/7/2023	https://VMware.zoom.us/rec/share/C-v5uu1nkFvrSonNJW04jFRnOQODgRnzSFILCR2kQvYsKEH81p33rl6CQHgk3dN.J9iB8MI-d2XS-h4a Passcode: fSnx.3Kk (Main topics: UX discussion on URL Reputation, URL Filtering DP behavior to enforce DPI for all web traffic)
11/29/2023	https://VMware.zoom.us/rec/share/8k3DBRqZYmNYrWbZ5B7sUUjDnxCljxgQCPB3NqRh9BGga40Zp586P5Hwi5EHH0Ld.yb9739k88H0zMgAT ⁵⁹ Passcode: 8zXH6\$do (Main topics: DP behavior w/ EFS configuration, Webroot SDK crash status)
2/27/2024	https://broadcom.zoom.us/rec/share/dlmpA37UF34n7zyl57MZn04EQjRtsQaaQ3hB0imQ7iL819NPgNVWhIN6VDKBAHW0.ui4D0S7I4M4s0LQm Passcode: &?*inv83 (Main topics: IDPS Memory Leak Issue, Request for Security Reporting PRD approval)
3/5/2024	https://broadcom.zoom.us/rec/share/xfajetCMkjinRcF2no6tzw_qz3-YPZh3kogj4LsGGGnYVezDDkS8FIBQKQoj5lpzV.fY1rz6dYy7aFYy3u ⁶⁰ Passcode: h5V=h33H (Main Topics: Security Reporting PRD Review)
3/12/24	https://broadcom.zoom.us/rec/share/lvcbvSU4n61KA2yiBLM9mgrBfVqDePS7zU3e_nLDhwwgbPVKEIWUqy77k20h8NNu.k5AAcXaX9f1DJp_n ⁶¹ Passcode: M%7Az5n% (Main Topics: Security Report PRD questions addressed, Inbound 1:1 NAT / Port Forwarding PRD review request)

⁵⁹ <https://vmware.zoom.us/rec/share/8k3DBRqZYmNYrWbZ5B7sUUjDnxCljxgQCPB3NqRh9BGga40Zp586P5Hwi5EHH0Ld.yb9739k88H0zMgAT>

⁶⁰ https://www.google.com/url?q=https://broadcom.zoom.us/rec/share/xfajetCMkjinRcF2no6tzw_qz3-YPZh3kogj4LsGGGnYVezDDkS8FIBQKQoj5lpzV.fY1rz6dYy7aFYy3u&source=gmail-imap&ust=1710265492000000&usg=AOvVaw0YpX7ttiTgIKvRoukwNr-6

⁶¹ https://www.google.com/url?q=https://broadcom.zoom.us/rec/share/lvcbvSU4n61KA2yiBLM9mgrBfVqDePS7zU3e_nLDhwwgbPVKEIWUqy77k20h8NNu.k5AAcXaX9f1DJp_n&source=gmail-imap&ust=1710863299000000&usg=AOvVaw0o8V4iDyq2Tfwi3GEaoYEv

19.5 UX VCE ATP Features Workshop (May 9th, 2022)

19.6 Parking Lot Questions