

תיאור פתרון ענן לגלישה מאובטחת

עבור

משרד החוץ



21 נובמבר 2017

לבקשתכם, חברת MedOne מתכבדת להציע למשרד החוץ פתרון ענן עבור גלישה מאובטחת בשיתוף פעולה עם אחד מספקי התוכנה SmartX או Crusoe Security.

הפתרון המוצע מבוסס על הענן המתקדם MedOneCloud מבית MedOne המסופק מתוך מתקני המחשב המאובטחים של MedOne בישראל. פתרון MedOneCloud מציע רמת זמינות ללא תחרות, שרות וסיוע טכני 24X7 בעברית והוא חלק מרשת בינלאומית של מתקני תשתית בענן OneCloud של חברת Dimension Data העולמית.

חברת MedOne בשיתוף עם חברת Dimension-Data הביאו לישראל את בשורת שרותי הענן הציבורי המתקדם ביותר בארץ.

במענה זה נפרט את יתרונות הפתרון המוצע, התאמתו למשרד החוץ על מכלול הצרכים המבצעיים משרות גלישה מאובטחת והצעת מחיר כוללת למימוש הפתרון בענן כשרות. תשתית הענן של MedOne מותקנת פיזית במתקני MedOne בישראל וכוללת:

- אירוח שרותי הענן במתחמים תת קרקעים המאובטחים ביותר העומדים בתקני משק לשעת חירום
- רמת הזמינות הגבוהה בישראל של שרותי הענן (עד 99.999% זמינות בשנה בשימוש בשני המתקנים)
- עמידה בתקני אבטחת מידע וברגולציות החמירות ביותר שיש
- קישוריות פנימית מאזור הארוח של מתקן הייצור של רינא מערכות לענן ללא עלות
- השגת זמני תגובה מעולים לחווית משתמש איכותית
- אפשרות ל"דלג" לאתר ענן בטירת הכרמל במקרה אסון באזור גוש דן

בברכה,

זרינה נישנוב | מנהלת מכירות

www.medone.com | zarinan@medone.com

טל. +972-9-7476008 | נייד +972-52-2221763 | פקס +972-9-7476011

תקנים והסמכות

	משק לשעת חירום		ISO27001 תקן למערכת ניהול אבטחת המידע בארגון
	תקן סליקה PCI		CSA STAR
	ISO27017 תקן למערכת ניהול אבטחת המידע בארגון		תקן ISO למידע רפואי בענן

פריסה עולמית יחודית



www.MedOne.com | info@MedOne.com

הנגר 6 א', הוד השרון | ת.ד. 466 4527704 | טל. 09-7476000 | פקס. 09-7476011

3. פתרון גלישה מאובטחת מבוסס טכנולוגיית Crusoe Security

קונספט הפתרון

Crusoe Security מקימה מערכת בענן MedOne לגלישה מאובטחת.

הפתרון הינו פתרון מלא מקצה לקצה וכולל את כל הרכיבים הרלוונטיים לשימוש בתהליך גלישה באינטרנט. רכיבים אלה כוללים גלישה, הורדה והעלאה של קבצים, הלבנה, סינון אתרים, אנטי וירוס, Load balancer וכו'.

יתרונות השימוש בענן:

1. אפשרות להפעלת המערכת לפי שימוש
2. קבלת שירותים נלווים מלאים על המערכת כגון מערכת הלבנה, Web filtering וכו'
3. אין צורך לרכוש חומרה ורישוי VMware וכו'
4. תשלום שכירות שנתי שכולל הכל (אין צורך ברכישות)
5. אחריות תחזוקת המערכת והשרתים הינה של Med One
6. זמינות הסביבה גם במקרה חירום (אתר DRP)
7. פריסה גלובלית בעולם

הנחות עבודה

8. אין התקנות בסניפים
9. כל התעבורה הסודית עוברת לפרוקסי ה LAN של משרד החוץ בישראל
10. סה"כ 98 נציגויות בעולם
11. בכל נציגות יש AD ready only
12. שימוש ב 4 Data Centers בעולם שימשו את כלל הנציגויות
13. שלב א' – 600 משתמשים שמיים
14. שלב ב' – 3000 משתמשים שמיים – 600 בו זמנית
15. סקר ביצועי תעבורה של MedOne – מסתמכים על הנתונים שבסדר לקביעת אתר ראשי ומשני לכל סניף. מה שמוגדר כטוב הוא פחות מ MS80.
16. הגלישה עצמה מכל נציגות מתרחשת ישירות ממחשב המשתמש בנציגות, למול חוות הגלישה הקרובה אליו
17. יש במשרד החוץ LB (עבור שרתי Proxy הפנימיים)
18. יש site to site בין העננים לבין עצמם, וגם site to site בין אתר ירושלים לכל העננים

תפיסת הפתרון:

1. הפתרון של Crusoe תומך בכל הפרוטוקולים – השימוש כברירת מחדל יהיה תמיד בפרוטוקול RDP של מיקרוסופט. במקרים בהם ה Latency עולה עם פרמטרים שיוגדרו, יבוצע שימוש בפרוטוקול של Citrix.
2. ישנם שני Data Centers מרכזיים (ישראל ואירופה) בהם יהיו כל השירותים (גלישה + הלבנה וכו')
3. ישנם שני Data Centers נוספים (ארה"ב והונג קונג) שהם יש שירותי גלישה בלבד
4. כל הרישוי (כולל RDP וכולל CITRIX) הוא רישום לפי משתמש (Named) ולא לפי כמות בו זמנית (Concurrent)
5. Web filtering – מערכת מבוססת Check Point אשר תיתן שירות בכל DC. הרישוי באחריות משרד החוץ.
6. מערכת הלבנה – מערכת מבוססת SASA אשר תיתן שירות לכל הקבצים שמשתמשים מורידים בסביבה. השירות הזה ינוהל בשני DC מרכזיים (ישראל ואירופה) וייתן שירות לכל המשתמשים של משרד החוץ. רישוי באחריות של משרד החוץ.
7. שרת קבצים – שרת שיתופי המשמש את כל המשתמשים. השירות הזה ינוהל בשני DC מרכזיים (ישראל ואירופה) וייתן שירות לכל המשתמשים של משרד החוץ. לכל עובד תהיה הרשאה לתיקייה הפרטית שלו בלבד.
8. Load Balancer – כשירות ענן

רכיבים On Premise:

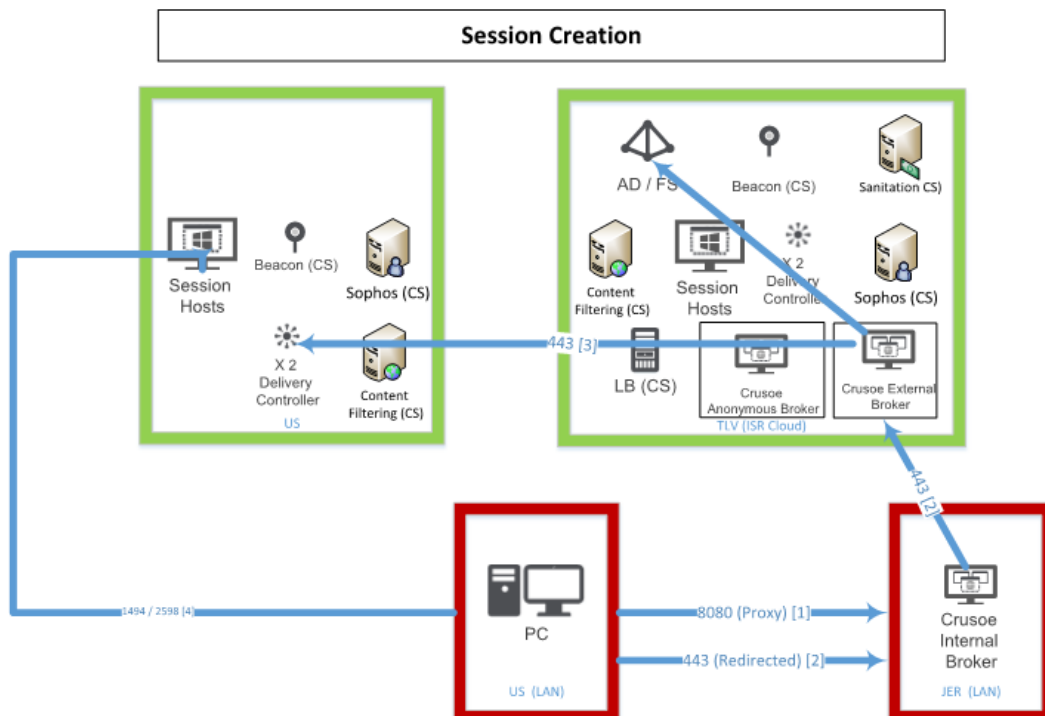
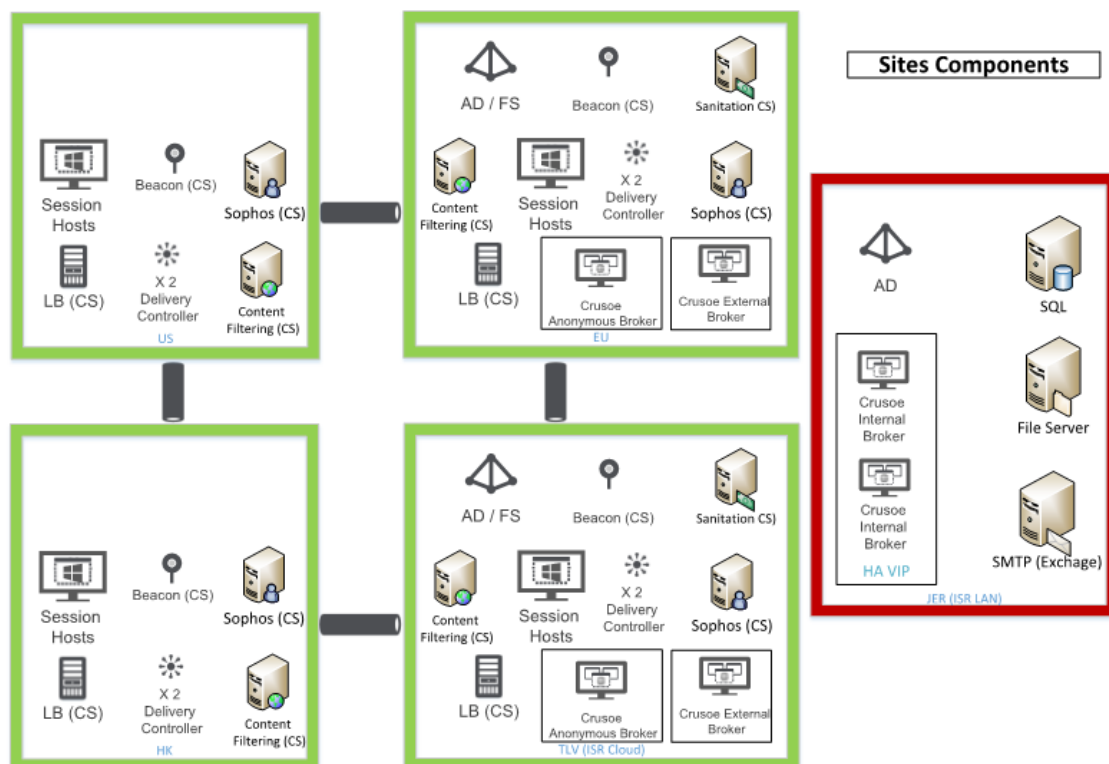
1. שרת Crusoe Internal – מספר שרתים (3-4) שמותקנים ב LAN של הלקוח ונותנים שירות לכל המשתמשים
2. LB – רכיב של משרד החוץ. שרתי Crusoe Internal ינוהלו מאחורי ה LB
3. SQL – רכיב של משרד החוץ. שרת Crusoe Internal מבצע רישום למסד הנתונים הזה.

המספרים המופיעים לעיל, הינם הערכה למשאבים הנדרשים לשימוש של 600 משתמשים (שלב א) בפריסה של ארבעת ה DC המצויינים לעיל.

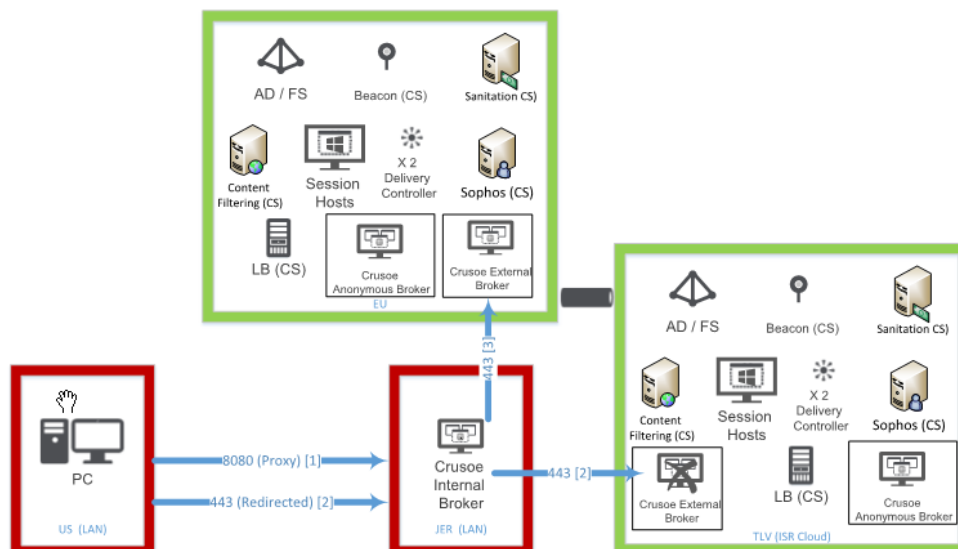
Datacenter	Server type	Quantity	VCPU	MEM	DISK	Hours	Backup
TLV	Management TS	1	1	2	50	730	yes
TLV	External	1	1	2	50	730	yes
TLV	Active Directory + File Server	1	2	4	100	730	yes
TLV	TS Master	1	4	12	50	730	yes
TLV	TS	2	4	12	50	210	
TLV	XenApp Master	1	4	16	50	730	yes
TLV	XenApp	1	4	16	50	210	
TLV	Crusoe Anaonymus broker	1	1	4	50	730	yes
TLV	Beacon	1	1	4	50	730	yes
TLV	Delivery controller	1	2	6	50	730	yes
TLV	Mail Snitation (LINUX)	1	1	2	50	730	
EU	Management TS	1	1	2	50	730	yes
EU	External	1	1	2	50	730	yes
EU	Active Directory + File Server	1	2	4	100	730	yes
EU	TS Master	1	4	12	50	730	yes
EU	TS	4	4	12	50	210	
EU	XenApp Master	1	4	16	50	730	yes
EU	XenApp	1	4	16	50	730	
EU	Crusoe Anaonymus broker	1	1	4	50	730	yes
EU	Beacon	1	1	4	50	730	yes
EU	Delivery controller	1	2	6	50	730	yes
EU	Mail Snitation (LINUX)	1	1	2	50	730	
US	TS Master	1	4	12	50	730	yes
US	TS	2	4	12	50	210	
US	XenApp Master	1	4	16	50	730	yes
US	XenApp	1	4	16	50	210	
US	Beacon	1	1	4	50	730	yes
HK	TS Master	1	4	12	50	730	yes
HK	TS	1	4	12	50	210	
HK	XenApp Master	1	4	16	50	730	yes
HK	XenApp	1	4	16	50	210	
HK	Beacon	1	1	4	50	730	yes

Data center	service	remarks
TLV	Sophos content filtering	for all TS+Citrix servers
HK	Sophos content filtering	for all TS+Citrix servers
EU	Sophos content filtering	for all TS+Citrix servers
US	Sophos content filtering	for all TS+Citrix servers
TLV	vlan	3
EU	vlan	3
HK	vlan	2
US	vlan	2
All	Anti Virus	For all servers
All	Backup	1.2 TB, 22 servers
All	Site to Site VPN between Datacenters	
All	Site to Site VPN between Jerusalem and all Datacenters	
All	Direct Line between Jerusalem and ISR cloud?	to be decided with Med One (can be SSL VPN)
All	Full System support	Installation, Patches, Monitoring, support etc.

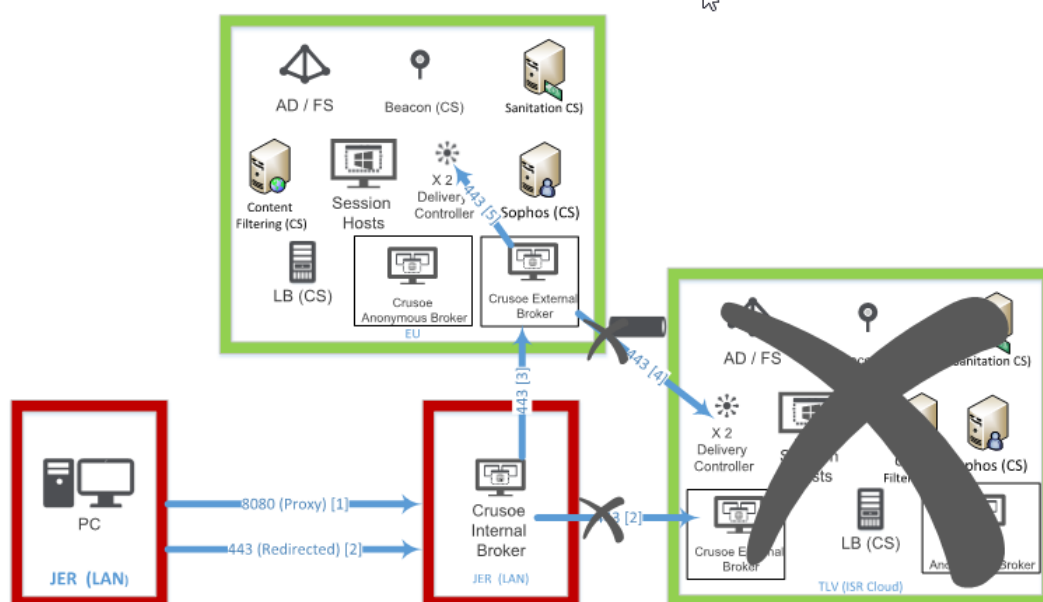
איורים סכמתיים של תפיסת הפתרון:



HA Topology – Crusoe External Broker Down



HA Topology – Israel Cloud Down



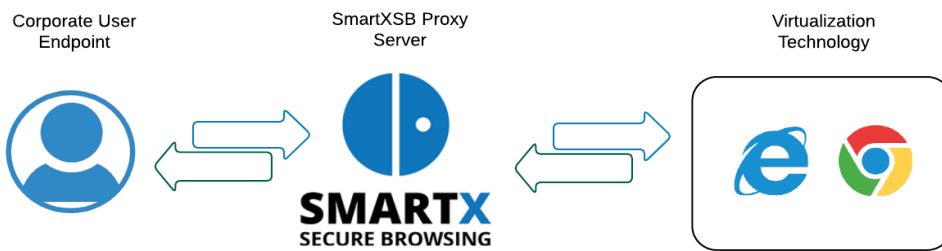
4. פתרון גלישה מאובטחת מבוסס טכנולוגית SmartX

פתרון הפרדת הגלישה הארגונית של סמרטאיקס מאפשר לארגונים לשמר את הפעילות העיסוקית שלהם באינטרנט ללא חשש של זליגת מידע ואיומים על המידע הרגיש בארגון. המוצר מבודד את הגלישה של המשתמשים הארגוניים לאתרים חיצוניים ואתרים פנימיים כך שכל איום על המידע הרגיש בארגון או בתחנת העבודה פשוט אינו קיים. הפתרון מאפשר גלישה על דפדפן חיצוני לארגון, ב-Cloud אשר נצפה ע"י המשתמש בתמונה. הפתרון מתממשק למערכות הלבנה שונות המאפשרות להכניס לארגון קבצים בצורה מאובטחת תוך שמירה על חוויית המשתמש אופטימלית.

מהות המוצר/ הפרויקט – SMARTX Secure Browsing

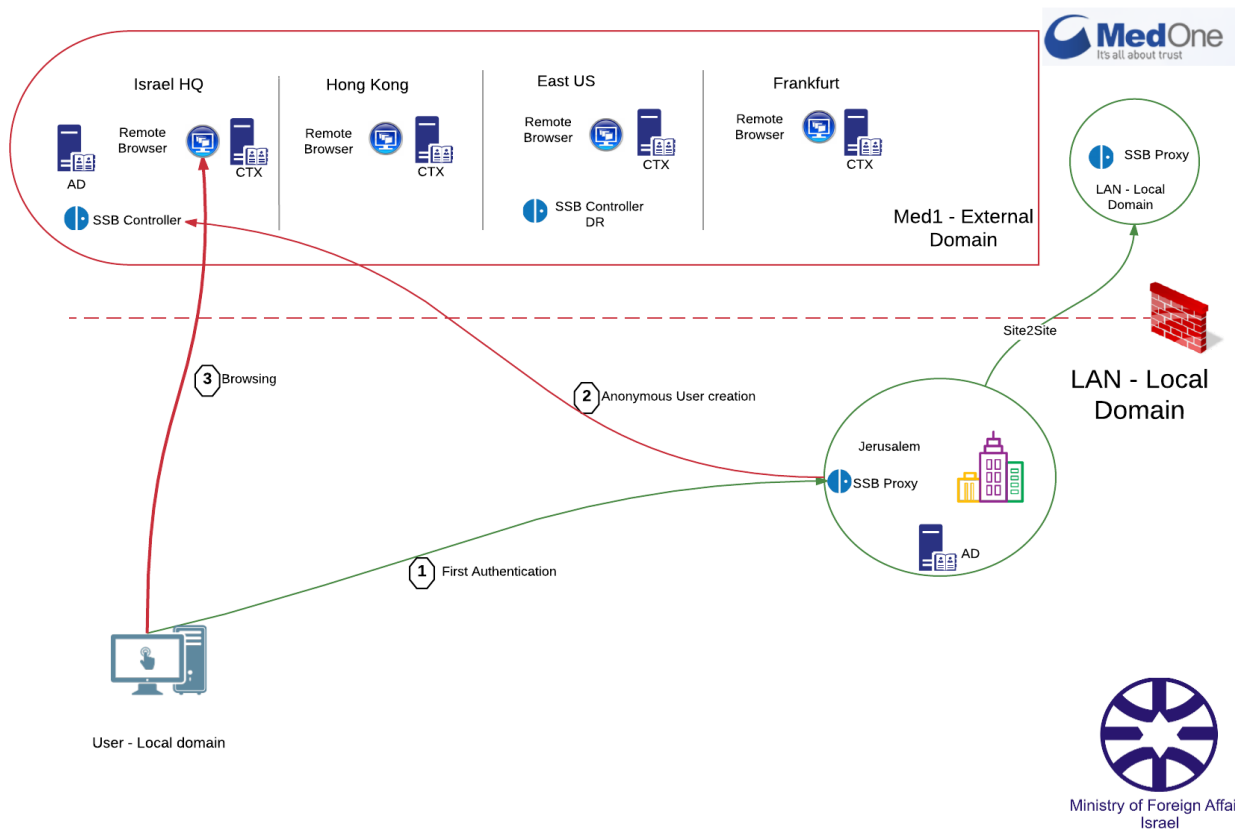
- הפרדה מוחלטת של הגלישה באינטרנט מה LAN של הארגון.
- מימוש וירטואליזציה של הגלישה באנטרנט ע"י תשתיות XenApp\XenDesktop\RDS\Horizon
- קיום שקיפות תפעולית מקסמלית למשתמש
 - o הזדהות וניהול (SSO מלא)
 - o הפעלות הדפדפן הרלוונטי (מקומי, וירטואלי, או אחר) בצורה אוטומטית
 - o עבודה ב Seamless window
 - o הורדת קבצים
- הפצת הקבצים הנדרשים אל משתמשי הקצה והנגשתם
- שליטה ובקרה מלאה על חוויית הגלישה של המשתמש
- מימוש מלא ע"ג תשתיות Remote Desktop Service
- התממשקות מלאה אל מערכות אבטחת המידע והלבנת הקבצים של הארגון
- התממשקות מלאה אל מערכות סינון התוכן והקניית זכויות הגלישה אל קבוצות משתמשי הארגון
- ניהול ע"י הקיים בארגון (אי יצירת ספריות משתמשים נוספות לניהול) ושקיפות תפעולית
- התממשקות ומתן כלים למיטוב דוחות גלישה

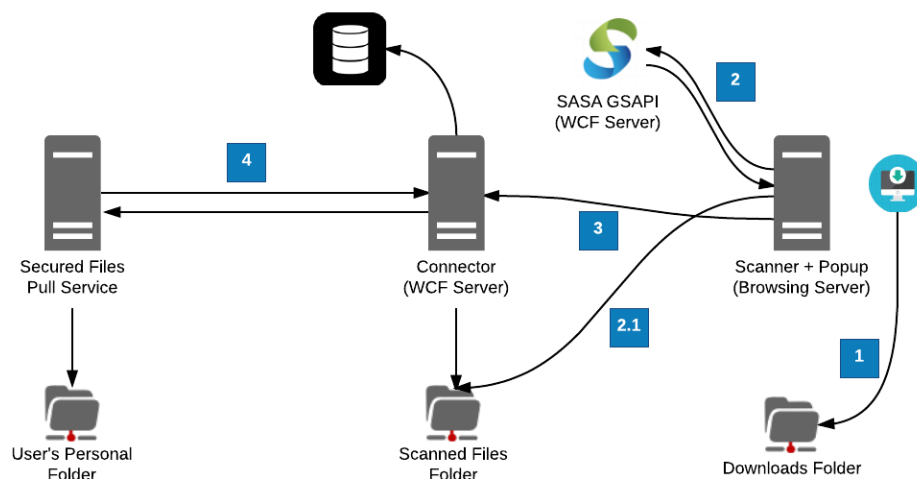
להלן תרשים לוגי של תהליך ההתחברות למערכת:



להלן תיאור ההתחברות של משתמש קצה לסביבת הגלישה:

1. בדפדפן של תחנת הקצה תוגדר הפנייה (Proxy Settings) לרשומה אשר מייצגת את שרת ה-SSB Proxy (שרת LAN) – ייושם על ידי GPO.
2. משתמש הקצה מפעיל דפדפן מקומי, במקרה שהאתר אליו ניגש המשתמש נמצא ב-White list של רכיב ה-SSB, הגלישה תמשיך מהדפדפן המקומי.
3. במקרה ומדובר באתר חיצוני, בשלב ראשון תתבצע בדיקה של שרת ה-SSB אם למשתמש הנ"ל קיים משתמש מקביל ב-Domain החיצוני של ה-SSB. במידה וכן, תתבצע הפעלה אוטומטית של HDX Seamless session מול חוות ה-CTX הייעודית שנמצאת בסביבת MedOne עם הזדהות של המשתמש המקביל (סיסמה רנדומאלית המחוללת על ידי רכיב ה-SSB) ולמשתמש אין אובייקט מקביל ב-Domain החיצוני, המערכת (SSB) תבצע הקמה (On the fly) של משתמש מקביל ב-Domain החיצוני ולאחר מכן תתבצע פתיחת ה-HDX session המשתמש חייב להזדהות לפחות פעם אחת כאשר הפרוקסי (On-Line).
4. ה-Seamless session שיופעל יפתח בסיום תהליך הכניסה חלון דפדפן המערכת תומכת במגוון סוגי דפדפנים (Chrome, IE, Firefox) וניתן לבצע שיוך של קבוצות ו\או משתמשים עבור פתיחה אוטומטית של סוג הדפדפן הרצוי.
5. המשתמש מבצע Authentication מול שרת ה-XenApp אליו הופנה המשתמש על ידי רכיב ה-CTX Broker. ההזדהות מתבצעת באופן שקוף לחלוטין בעזרת SSO מובנה של הפתרון.





- 1** User is downloading a file in the browsing session, the file is being sent to SASA content inspection system, Progress bar appears.
- 2** SASA's GateScanner is checking the file and return a stream of a new 'secured' file
- 3** The 'Secured' file is being sent to the SSB Connector which saves the file to the scanned files folder and records it in the database.
- 4** The Pull Service query the Connector for new scanned files, if there are new files, it verifies their hash, if it matches it pulls them into the internal environment and saves them to the end user personal folder

להלן דרישות החומרה

להלן טבלה עם דרישות החומרה עבור הפתרון הכולל:

מס"ד	שם השרת (זמני)	תפקיד השרת	OS	מעבד	זיכרון	כמות	גודל דיסק	מיקום
1.	SSB01	SSB Secure Browsing Controller	Windows 2012 R2	2 vCPU	8GB	2	50GB	MOFA DC - LAN

סביבה LAN – שרתים ב-Domain הפנימי (דרישות חומרה וירטואלית מהלקוח)

Management (Med1- Israel) – שרתים ב-Domain החיצוני

Number of Servers	OS	Storage	RAM	CPU	Server Role
2	Windows 2012 R2	50 GB Drive C	8 GB	4 VCPU's	SQL + Citrix Management
2	Windows 2012 R2	100 GB Drive	12 GB	4 VCPU's	AD External + SSB Controller + Filer
4		50 GB Drive C	6 GB	4 VCPU's	SASA Servers
2		100 GB Drive C	8 GB	4 VCPU's	SASA MNG

(Med1 Israel) – שרתי גלישה ב-Domain החיצוני

Number of Users	Number of Servers	OS	Storage	RAM	CPU	Server Role
144	4+1	Windows 2012 R2	50 GB Drive C	24 GB	6 VCPU's	TS
	2	Windows 2012 R2	50 GB Drive C	6 GB	2 VCPU's	AD + Filer

(Med1 Frankfurt) – שרתי גלישה ב-Domain החיצוני

Number of Users	Number of Servers	OS	Storage	RAM	CPU	Server Role
222	6+1	Windows 2012 R2	50 GB Drive C	24 GB	6 VCPU's	Frankfurt
	2	Windows 2012 R2	50 GB Drive C	6 GB	2 VCPU's	AD + Filer

(Med1 Hong Kong) – שרתי גלישה ב-Domain החיצוני

Number of Users	Number of Servers	OS	Storage	RAM	CPU	Server Role
92	4+1	Windows 2012 R2	50 GB Drive C	24 GB	6 VCPU's	TS
	2	Windows 2012 R2	50 GB Drive C	6 GB	6 VCPU's	AD + Filer

(Med1 East US) – שרתי גלישה ב-Domain החיצוני

Number of Users	Number of Servers	OS	Storage	RAM	CPU	Server Role
128	4+1	Windows 2012 R2	50 GB Drive C	24 GB	6 VCPU's	TS
	1	Windows 2012 R2	50 GB Drive C	6 GB	2 VCPU's	AD + Filer

- שרת עם קישור ל**DB** המרכזי (או לחליפין ניתן להתקין שרת **DB** ייעודי או מקומי על השרת פרוקסי).
- אספקת רישוי RDS CAL עבור X משתמשים (כמות המשתמשים אשר תיבדק).
- אספקת רשימת קבוצות מנוהלות ב URL Filtering ויש לסנכרן מה Domain הפנימי ל Domain הפיקטיבי.
- פתיחת פורטים נדרשים על פי הטבלה להלן:

Source	Destination	Port
User Client	External Citrix	TCP 1494/2598
User Client	SSB - LAN	TCP 8081/443
User Client	Filer - LAN	SMB
LAN SSB	Domain Controller - LAN	TCP 389/636/53
Med-1 SSB	External Domain Controller	TCP 389/636/53
LAN SSB	External SSB	TCP 8878
SSB LAN	FS - LAN	SMB
LAN SSB	DB	TCP 1443

הלבנת קבצים

הפתרון כולל שירות הלבנת קבצים מבית Sasa הכולל file recreation, חתימות אנטי וירוס ועוד סריקות הרישוי באחריות משרד החוץ

URL Filtering

הפתרון כולל שירותי Url filtering מסוג Sophos הכוללים סינון אתרים על פי קטגוריות. הרישוי באחריות MedOne