Top Benefits of Isolated Remote Browsing

The internet presents workers with unprecedented access to an incomparable wealth of resources. But it also presents unprecedented risk to every organization. A single user browsing the internet can unintentionally place an organization's most sensitive corporate assets at great risk. Multiply that single user by tens, hundreds or thousands of users and the risks that face today's organizations through employee internet access are nearly incalculable.

Many organizations have attempted to mitigate that risk by using remote browsers enabled by Citrix products. But remote browsing simply does not provide a sufficient safeguard; isolating browsing from the corporate network is the only true defense against the many internet-based security risks that seek to breach vital corporate systems and data.

This paper discusses the benefits of browser isolation. It also spotlights a way to isolate corporate users from internet threats by executing all external content on an isolated remote browser — sending the user a safe, malware-free version of the stream. It further discusses the integration of SmartX Secure Browsing (SmartXSB) with Citrix in providing a secure remote browsing experience for corporate users.

Business Challenge Summary

In 2010, one of the world's largest and most sophisticated technology companies, Google, announced that it had been the victim of an organized group of hackers based in China. The successful attack harvested vast quantities of highly sensitive U.S. Government data by breaching a Gmail database. Yahoo, Adobe and dozens of additional companies were attacked simultaneously by the same group. The incident is now ranked as one of the worst hacking attacks in history, according to *Wired*.

How did hackers so easily breach the defenses of many of the most technologically advanced, security-conscious companies on the planet? They leveraged security flaws in older versions of Internet Explorer web browsers used by employees.

Breaching enterprise defenses through web browser vulnerabilities is, in fact, a tactic cybercriminals consistently deploy. Breaches often occur when employees use older versions of web browsers containing known security flaws. It happens with great regularity. In just the first quarter of 2016, 48 percent of all malicious cyberattacks occurred via email attachments, many directing unsuspecting users to malicious URLs, infected websites, and leveraging browser vulnerabilities.

Keeping all employees up to date with the latest, most secure web browsers have failed. And many in-house websites are not kept compatible with newer browsers — often the result of in-office red tape. The reality is that across thousands of enterprises worldwide, employees routinely use a mix of web browser versions, many of them old and obsolete. The resulting array of security vulnerabilities coalesce to present a prime target for cybercriminals.

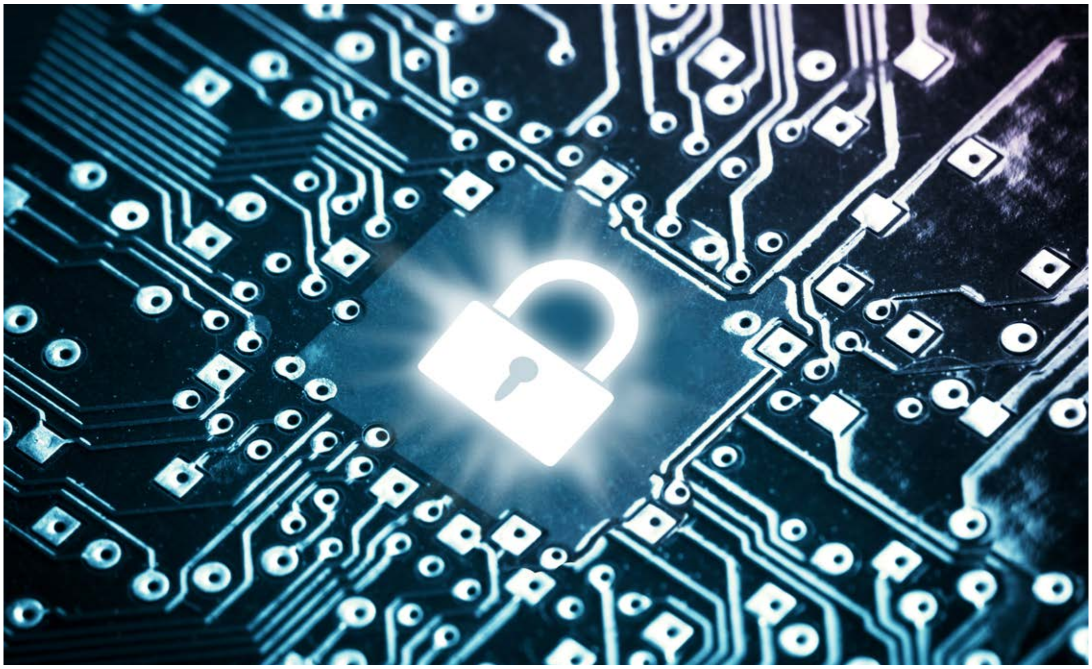
Gartner's report, *It's Time to Isolate Your Users from the Internet Cesspool with Remote Browsing*, notes that deploying a remote browser solution is "one of the most significant ways an enterprise can reduce the ability of web-based attacks on users to cause damage." The report also forecasts that 50 percent of all enterprises will actively implement solutions to isolate internet browsing by 2021, a radical increase from the less than five percent of companies deploying secure browsing solutions in 2016.

But the rampant security vulnerabilities posed by web browsing are not entirely eliminated through remote browsing. Malware and ransomware may still find and exploit many browser-based points of weakness. The only way to effectively eliminate these security threats is to completely isolate browsing from the corporate network through a fully managed secure browsing solution.

A number of issues contribute to the rise of insecure browsing.

- URL filtering is not 100 percent accurate
- Websites can infect visitors
- They cannot stop malicious files
- Web gateways cannot isolate malware

Another solution must be found.



Top Seven Features to Consider in a Secure Browsing Solution

Maximizing the benefits of a secure browsing solution requires the installation of a system that delivers a full range of key capability and usability features. The following, in particular, should be considered must-have features for secure browsing solutions undergoing evaluation for deployment in any organization:

1. **Browsing Policy Enforcement:** Virtually every enterprise on the planet has implemented policies that dictate employees' activities and actions regarding internet access. These policies are designed, at least in part, to help prevent the occurrence of browser-based security breaches. Many organizations, however, do not actively enforce the policies, rendering the policies effectively worthless in providing a form of defense. A secure browsing solution should enable and facilitate the universal enforcement of organizational browsing policies.
2. **Seamless User Experience:** From the user's perspective, secure browsing should be transparent. The experience should be identical to using a desktop-based browser. It is particularly crucial that the secure browsing solution enable personalization in a single-browser environment.
3. **User Identity Protection and Management:** The solution should anonymously shadow user's protection.
4. **Browsing Performance Utilization:** Though browser performance can suffer with some remote solutions, a secure solution should ideally enable performance that is on par with desktop-based browsers. Some secure browsing solutions can even enhance browsing performance by facilitating a range of cloud and on-premise options for accessing different websites securely. The best, safest platform should be automatically determined for URLs, users and location-based prioritization and scheduling management.
5. **Cloud Internet Browsing:** Maximum efficiency and user productivity are facilitated with solutions that enable internet browsing on any cloud system or data center.
6. **Browser Compatibility:** The solution should enable the use of a single browser for all different applications and URLs.
7. **Regulatory Compliance:** The ability to maintain 100 percent separation between the internet and sensitive enterprise data is a good policy for all companies, and a regulatory necessity for many companies.

Citrix Ready Secure Remote Access Program Overview

Citrix solutions deliver a complete portfolio of products supporting the secure access of apps and data anytime, at any place, on any device and on any network. These include:

1. XenApp and XenDesktop to manage apps and desktops centrally inside the data center
2. XenMobile to secure mobile applications and devices while providing a great user experience
3. ShareFile to provide controlled and audited data access, storage and sharing, both on-premise and in the cloud
4. NetScaler to contextualize and control connectivity with end-to-end system and user visibility

CITRIX XenDesktop

CITRIX XenApp

CITRIX XenMobile

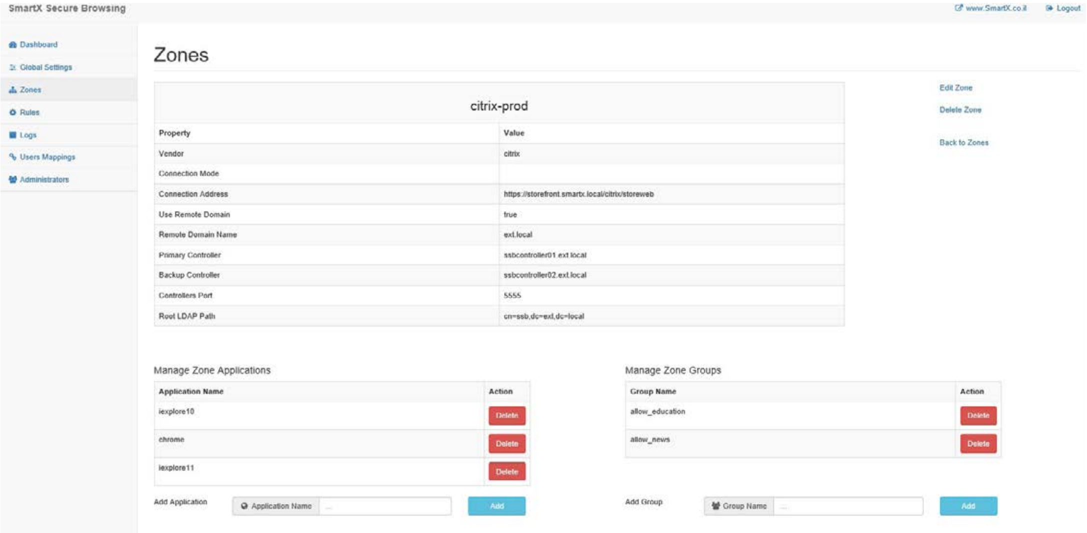
CITRIX ShareFile

CITRIX NetScaler

Citrix solutions also integrate with third-party security products to provide advanced levels of system management and identity, endpoint and network protection. The Citrix Ready Secure Remote Access program was launched to identify and showcase partner products that are proven to smoothly integrate with Citrix products, and that work to enhance Secure Remote Access by adding extra layers of security. The Citrix Ready Secure Remote Access program serves as an aid to IT executives in quickly and easily finding and sourcing solutions for their Secure Remote Access needs, helping to secure organizations' corporate networks from theft of data, DDoS and other security attacks that may be perpetuated via Remote Access.

Citrix advises that organizations can best defend against security attacks that might occur through Remote Access by following five best practices — pillars of focus that support enterprise security:

1. **Identity and Access**: Administrators must be able to confirm the identity of users requesting access to a system and limit the degree of access granted. In comparison to simple password-based systems, two-factor authentication offers a vast improvement in the ability to properly confirm user identity in requests for access. The degree of access granted to each individual user should be based on context. The principle of least privilege helps to ensure that users are granted rights that are limited only to those required in the performance of their jobs.
2. **Network Security:** The growing demand for remote access complicates the process of securing a network. Yet the integrity of network security must be maintained while supporting remote access for mobile and third-party users. Network and host segmentation can be useful in shrinking surfaces that are vulnerable to attack. And implementing a multilayer approach helps to boost network security while ensuring availability.
3. **Application Security:** All types of applications are potential targets for hackers, but the veritable explosion of apps has created many additional points of vulnerability for most enterprises. Apps on mobile devices are particularly susceptible to exploitation. An important step in reducing risk is enacting centralization and the encrypted delivery of applications. Containerization for mobile apps and inspection of incoming data streams can help to reduce app-related security vulnerabilities.
4. **Data Security:** The security of enterprise data can be enhanced by the centralization and hosted delivery of data by enforcing secure file sharing (to reduce data loss) and by the containerization of data (both in-transit and at rest).
5. **Monitoring and Response:** Vigilance and fast action are required to successfully counter the attacks that most enterprises face on a daily basis. A rapid response to breaches is also critically important, given that even the most secure systems are vulnerable to successful attacks. Rapid detection and response to successful attacks serve to minimize damage and limit susceptibility to additional attacks. End-to-end visibility into application traffic supports faster identification of security breaches and system anomalies.



Zones

citrix-prod

Property	Value
Vendor	citrix
Connection Mode	
Connection Address	https://storefront.smartx.local/citrix/storeweb
Use Remote Domain	true
Remote Domain Name	ext.local
Primary Controller	ssbcontroller01.ext.local
Backup Controller	ssbcontroller02.ext.local
Controllers Port	5555
Root LDAP Path	cn=ssb,dc=ext,dc=local

Manage Zone Applications

Application Name	Action
iexplore10	Delete
chrome	Delete
iexplore11	Delete

Manage Zone Groups

Group Name	Action
allow_education	Delete
allow_news	Delete

The Benefits and Burdens of Remote Access

Remote access has enabled an entirely new paradigm of workplace flexibility and productivity. Indeed, the very meaning of the word “workplace” must be redefined to be less location specific, and more worker specific. The adoption of mobility enhancing tools such as tablets, smartphones and other devices has transformed many enterprise roles into an any place, any time proposition. Workers have benefited from schedules that offer more flexibility, helping to enhance both work and home life. Companies have benefited from the leaps of productivity that remote access enables.

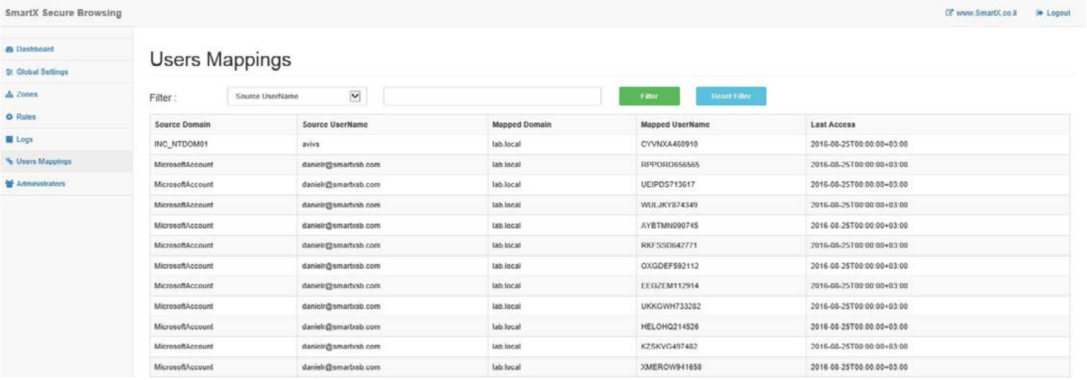
But this ongoing paradigm shift has required that enterprises find ways to balance the protection of sensitive data with the impact of remote access upon user flexibility — the widespread use of virtual public networks (VPNs) over unsecured networks, for example.

While remote access does increase the burden of safeguarding enterprise systems and data, the benefits of remote access justify the need for increased focus on security. The Citrix Ready Secure Remote Access program is designed to help enterprises conform to the five security pillars listed above while meeting the skyrocketing demand for more remote access capabilities.

SmartXSB has been selected to participate in the Citrix Ready Secure Remote Access program. SmartXSB’s secure remote browsing solution has demonstrated the ability to consistently support the five security pillars of the Secure Remote Access program.

Key features of SmartXSB include:

- **Complete User Privacy:** Though users may sometimes feel as if they are browsing the internet with complete anonymity, that is rarely the case with standard browsers. But SmartXSB completely protects the anonymity of users by creating a temporary anonymous user for a browsing session. The anonymous user is created in a different Active Directory forest, and is generated to represent only users browsing the internet or external environments.



Users Mappings

Source Domain	Source UserName	Mapped Domain	Mapped UserName	Last Access
INC_NTDOM01	avivs	lab.local	CYVNXA460910	2016-08-25T00:00:00+03:00
MicrosoftAccount	danielr@smartxsb.com	lab.local	RPPORO656565	2016-08-25T00:00:00+03:00
MicrosoftAccount	danielr@smartxsb.com	lab.local	UEIPDS713617	2016-08-25T00:00:00+03:00
MicrosoftAccount	danielr@smartxsb.com	lab.local	WULJKY874349	2016-08-25T00:00:00+03:00
MicrosoftAccount	danielr@smartxsb.com	lab.local	AYBTMN090745	2016-08-25T00:00:00+03:00
MicrosoftAccount	danielr@smartxsb.com	lab.local	RKFSSD642771	2016-08-25T00:00:00+03:00
MicrosoftAccount	danielr@smartxsb.com	lab.local	OXGDEF592112	2016-08-25T00:00:00+03:00
MicrosoftAccount	danielr@smartxsb.com	lab.local	EEGZEM112914	2016-08-25T00:00:00+03:00
MicrosoftAccount	danielr@smartxsb.com	lab.local	UKKGWH733282	2016-08-25T00:00:00+03:00
MicrosoftAccount	danielr@smartxsb.com	lab.local	HELOHQ214526	2016-08-25T00:00:00+03:00
MicrosoftAccount	danielr@smartxsb.com	lab.local	KZSKVG497482	2016-08-25T00:00:00+03:00
MicrosoftAccount	danielr@smartxsb.com	lab.local	XMEROW941658	2016-08-25T00:00:00+03:00

- **Straightforward Browser Management:** SmartXSB provides many features that work to simplify administrative browser management.
- **Convenient Single-Sign-On Capability:** Users are offered the convenience of logging in with a single set of credentials for access to all browsers and applications.
- **Consistently Holistic User Experience:** SmartXSB consistently provides a user experience that is convenient, fast and transparent in addition to the behind-the-scenes benefits of safer, more secure interfacing with external resources.
- **Total File and Clipboard Security Management:** SmartXSB mitigates the security risk represented by downloaded files and browser content copied to clipboards.
- **Perfect Integration with Content Inspection Systems:** SmartXSB integrates content inspection systems, giving them control over all browsing security-related areas of concern, including file security, URL filtering, known malware scans and more.

Overview of SmartXSB

SmartX Secure Browsing is a leading provider of secure remote browsing solutions. Its secure remote browsing solution enables a fast, secure and more efficient way for employees to access any website with confident. Any cyber threat is isolated so users and network remain safe and regulatory complied.

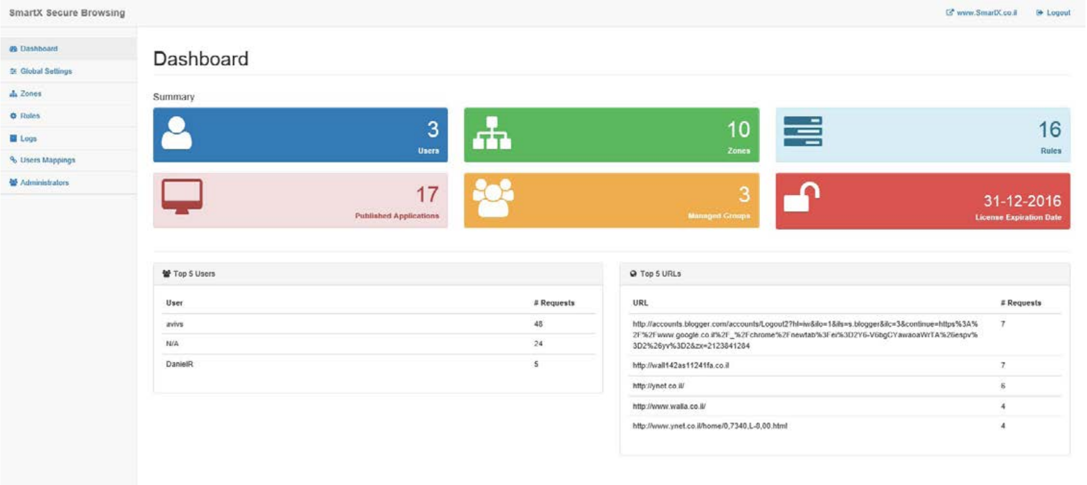
SmartXSB strengthens enterprise security through a substantial range of features, including:

- Enhanced User Privacy
- Single Sign-On Capability
- Integration with Content Inspection Systems

File security is strengthened through the uploading and downloading of files. SmartXSB also supports integration with a variety of third-party tools that enable file scanning and downloading in accordance with ICAP protocol.

SmartXSB's URL filtering capabilities allow administrators to control access to websites by permitting or denying access to specific websites according to pre-defined website categorizations. URL access scheduling supports IT security and access control policies. This allows admins to define the URL applications that are available to specific users at pre-defined times, and through specifically designated virtual machines or locations.

Notably, SmartXSB enables the safe browsing of external websites while simultaneously maintaining a streamlined, fast and fluid user experience. Users can migrate between different browsers with complete ease, setting and keeping their browser preferences while visiting whatever sites they desire — all while enjoying a lightning-fast, completely secure session. Security is enhanced without the diminishment of user productivity.



Dashboard

Summary

3 Users

10 Zones

16 Rules

17 Published Applications

3 Managed Groups

31-12-2016 License Expiration Date

Top 5 Users

User	# Requests
avivs	48
N/A	24
DanielR	5

Top 5 URLs

URL	# Requests
http://accounts.blogger.com/accounts/Logout2?hl=iw&ilo=1&ils=s.blogger&ilc=3&continue=https%3A%2F%2Fwww.google.co.il%2F_%2Fchrome%2Fnewtab%3Fei%3D2Y6-V6bgCYawaoaWrTA%26espv%3D2%26yv%3D2&zx=2123841284	7
http://wall142as11241fa.co.il	7
http://ynet.co.il/	6
http://www.walla.co.il/	4
http://www.ynet.co.il/home/0,7340,L-8,00.html	4

SmartXSB also provides advanced browsers management and compatibility control, providing administrators with the ability to fully regulate and manage organizational browsing policies — for all browser types and versions. The following tool sets and features enable the advanced managerial control provided by SmartXSB:

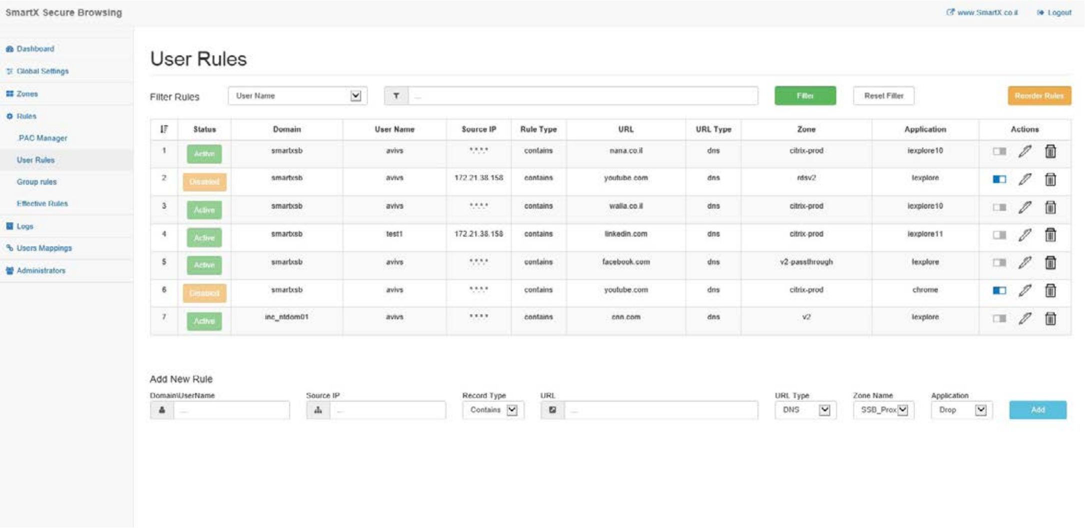
- User identity management
- Rule-based engine for facilitating the management of user locations, URL destinations, apps, timeframes and browser types and versions
- Multi-tenancy support
- User personalization support
- Multi-zone support

In sum, SmartXSB offers a complete package that combines browsing security with flawless performance, even when users visit the internet's most bandwidth-consuming websites. The ability for users to visit websites from different browser locations — cloud-based or even desktop-based — helps assure that both local PC-based and organizational network-based core applications will run faster.

SmartXSB is a Citrix Ready partner and has worked hand-in-hand with Citrix to provide companies with the ability to protect themselves and their employees from browser-based malware attacks and data breaches. As a member of the Citrix Ready program, SmartXSB has completed a comprehensive program of verification testing and has earned Citrix's complete trust in its ability to enhance the Citrix Delivery Center infrastructure.

SmartXSB's secure remote browsing solution offers a substantial range of unique benefits that competing products simply cannot match. SmartXSB:

- **Secures** browsing and browser management capabilities (URLs, users and location-based prioritization and scheduling management) for Citrix XenApp and XenDesktop for avoidance of malware/ransomware threats
- **Provides** a transparent browser user experience along with enhanced performance for corporate users
- **Controls** and manages every browser session launch according to the URL severity level
- **Supports** organizational browsing policy enforcement, assuring that each user, session, VDI zone and URL category will be aligned with corporate security requirements
- **Builds** a secure browsing environment, either on-premise or by using Citrix to enable safe cloud-based browsing
- **Accelerates** local PC environments by managing the target URL launching location, reducing overhead on the core application performance



User Rules

Filter Rules: User Name

	Status	Domain	User Name	Source IP	Rule Type	URL	URL Type	Zone	Application	Actions
1	Active	smartxsb	avivs	*.*.*.*	contains	nana.co.il	dns	citrix-prod	iexplore10	
2	Disabled	smartxsb	avivs	172.21.38.158	contains	youtube.com	dns	rdsv2	iexplore	
3	Active	smartxsb	avivs	*.*.*.*	contains	walla.co.il	dns	citrix-prod	iexplore10	
4	Active	smartxsb	test1	172.21.38.158	contains	linkedin.com	dns	citrix-prod	iexplore11	
5	Active	smartxsb	avivs	*.*.*.*	contains	facebook.com	dns	v2-passthrough	iexplore	
6	Disabled	smartxsb	avivs	*.*.*.*	contains	youtube.com	dns	citrix-prod	chrome	
7	Active	inc_ntdom01	avivs	*.*.*.*	contains	cnn.com	dns	v2	iexplore	

Add New Rule

Domain\UserName: ...
Source IP: ...
Record Type: Contains
URL: ...
URL Type: DNS
Zone Name: SSB_Prox
Application: Drop

SmartXSB Solution Detail

SmartXSB serves as a web proxy between Citrix users and their virtual environment, and can be implemented internally or on the cloud. All web content execution is controlled and isolated using SmartXSB's advanced rule engine, which determines where and how web content is displayed and which browser is used. The rule engine can be used to enhance organizational browsing policy, and provides managerial control over the websites that individual users are permitted to visit based on user privilege, user location and the requesting website.

External content is executed outside of and isolated from the corporate network, providing a safety buffer that assures all malware is effectively blocked from running internally. Traffic entering a secured internal network is limited to screen updates, prints and clipboard items. Internal networks remain secured and isolated, significantly reducing organizational vulnerabilities and exponentially shrinking the attack surface that may be targeted by cybercriminals.

SmartXSB permits users to interact with the internet's most bandwidth-intensive websites while accessing them from different browser locations. The resulting increase in operational efficiencies will assure that both local PC-based and organizational network-based core applications will run faster, boosting user productivity while simultaneously enhancing security.

A Proven Partnership that Helps Organizations Eliminate a Dangerous Vulnerability

Though most organizations are taking significant strides to protect themselves against the unprecedented and accelerating onslaught of cybercrime, few organizations are sufficiently addressing the gaping security hole that exists in many companies: browser security.

So pressing is the need for remote browser security that Gartner has identified it as a top 10 technology for information security. According to Gartner, "Most attacks start by targeting end-users with malware delivered via email, URLs or malicious websites. An emerging approach to address this risk is to remotely present the browser session from a 'browser server' ...running on premises or delivered as a cloud-based service. By isolating the browsing function from the rest of the endpoint and corporate network, malware is kept off of the end-user's system and the enterprise has significantly reduced the surface area for attack."

SmartXSB provides the ultimate secure remote browsing solution for Citrix users, empowering organizations with the ability to keep applications and data safe. But unlike many remote browsing solutions, SmartXSB does not impose constraints that serve to diminish user productivity. Instead, SmartXSB works to enhance productivity while simultaneously strengthening security — in effect, making the vast resources of the internet available to every user while filtering out the many inherent risks.

SmartXSB is proven to integrate seamlessly and easily with Citrix systems to provide an unbeatable secure, isolated remote browsing solution. SmartXSB's selection to the Citrix Ready Secure Remote Access program provides enterprises with a proven, reliable solution for facing the ever-escalating security needs of the modern business environment. For companies seeking to protect themselves against the modern-day scourge of cybercrime, the partnership of Citrix and SmartXSB offers an affordable, flexible, proven resource for enhanced security.

For more information about SmartXSB, please visit: http://smartxsb.com/

For more information about Citrix NetScaler, please visit:
https://www.citrix.com/products/netscaler-adc/

Appendix

Learn more about the enterprise security advantages provided by Citrix NetScaler Unified Gateway at: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/best-practices-for-enterprise-security.pdf

To learn more details about how SmartXSB enhances enterprise security, please visit: http://smartxsb.com/product

To learn more about using Citrix XenApp and Citrix XenDesktop for secure remote browsing, please visit: http://smartxsb.com/wp-content/uploads/2016/06/SmartX_Howto_v2-Final.pdf

To learn more about the Citrix Ready Program partnership with SmartXSB, please visit: https://citrixready.citrix.com/smart-x-professional-services-ltd.html

To learn more about security solutions for business enterprises, contact Citrix and SmartXSB.

About Citrix Ready
Citrix Ready identifies recommended solutions that are trusted to enhance the Citrix Delivery Center infrastructure. All products featured in Citrix Ready have completed verification testing, thereby providing confidence in joint solution compatibility. Leveraging its industry-leading alliances and partner ecosystem, Citrix Ready showcases select trusted solutions designed to meet a variety of business needs. Through the online catalog and Citrix Ready branding program, you can easily find and build a trusted infrastructure. Citrix Ready not only demonstrates current mutual product compatibility, but through continued industry relationships also ensures future interoperability. Learn more at citrixready.citrix.com.

About SmartX Secure Browsing
SmartX Secure Browsing is a leading provider of Secure Remote Browsing solutions. SmartXSB's browsing policy enforcement, user identity protection, browser compatibility, browsing performance utilization, and seamless user experience solutions enable a fast, secure and more efficient way for employees to access safely any website that might be infected with malware or ransomware. Any and every cyber threat is isolated so your users and your network remain safe and in compliance. Learn more at http://smartxsb.com.