
Citrix NetScaler Secure Web Gateway

With the exponential growth in web traffic and SaaS apps, customers need complete visibility and control over their web traffic. This includes visibility into encrypted traffic that helps customers to apply their corporate policies and block malicious content to protect their users and endpoints.

Encryption protects the privacy and integrity of data. Encryption also creates blind spots that attackers can exploit to evade security controls. Over half of all internet traffic today is encrypted, which creates a rather large gap in an organization's security posture, leading to increased vulnerability, risk, and possibly a damaged reputation. SSL decryption is a key component of NetScaler Secure Web Gateway (NetScaler SWG), a solution that enables organizations to cost-effectively eliminate blind spots within their environment and strengthen their security posture. With NetScaler SWG, organizations have the visibility and control they need over encrypted traffic to ensure compliance with their privacy, regulatory, and acceptable user policies.

Addressing security challenges

Organizations rely on a wide array of security products to inspect traffic, block intrusions, stop malware, and control which applications users can access. To keep users safe inside an organization, these products must inspect all communications, not just clear-text traffic. Many security devices are not designed for high-speed SSL decryption. Without SSL inspection, organizations are at risk from attacks. Hackers can infiltrate networks, install malware, and steal data across multiple endpoints in the guise of encrypted traffic.

Organizations need to inspect outbound SSL traffic originating from internal users.

NetScaler SWG is uniquely positioned in the network to help organizations achieve high-capacity, high-performing web security.

High-speed SSL decryption

Inspecting encrypted traffic is no longer optional. Increasing use of HTTPS as the default transport protocol means that administrators must be able to crack open these connections for inspection.

Purpose-built NetScaler SWG appliances help decrypt and encrypt traffic at high speed, and apply corporate policies. It allows customers to eliminate blind spots caused by SSL encryption.

Maintaining compliance

NetScaler SWG aids security teams in conforming to governmental privacy regulations and industry mandates. For example, organizations subject to the Children's Internet Protection Act (CIPA) can achieve compliance with NetScaler SWG, thus blocking websites unsuitable for schools and universities. In order to meet compliance requirements and ensure data privacy, NetScaler SWG will bypass sensitive communications such as traffic to banking and healthcare applications.

Organizations can now have the visibility and control they need over encrypted traffic while ensuring compliance with their privacy, regulatory, and acceptable use policies.

Achieve high performance with SSL acceleration hardware.

A purpose-built NetScaler SWG appliance equipped with powerful, dedicated SSL processors that can scale to handle up to 80,000+ 2048-bit SSL handshakes per second.

Selectively decrypt traffic.

NetScaler SWG allows for policy-based bypass according to URL category, URL reputation, or a customer list. For example, it bypasses trusted communication with banking or healthcare applications to meet compliance requirements.

Block malicious websites.

The NetScaler SWG URL Threat Intelligence Subscription service blocks access to malicious websites such as malware, spam, and phishing sites, which increases employee productivity and reduces business security risks.

NetScaler SWG can be used to prevent or limit access to services such as social networking, online auctions, online gambling, adult sites, personal web-based email, and celebrity gossip sites, thereby increasing employee productivity.

Access User Behavior Analytics.

Security operations teams gain deep visibility and real-time user behavior analytics to protect against malware threats.

Utilize actionable business value dashboard.

NetScaler SWG integrated with NetScaler Management and Analytics System (NetScaler MAS) provides security operations teams with NetScaler MAS analytics, visibility, and reporting across various network touch points and user data.

NetScaler URL Threat Intelligence Subscription

The NetScaler URL Threat Intelligence Subscription service is a real-time cloud-based solution that blocks access to millions of malware and phishing websites.

Customers can enable granular filtering on the NetScaler URL Threat Intelligence Subscription based on URL category and reputation.

Security operations teams can enforce corporate security policies on all outgoing web traffic while blocking access to inappropriate sites on a per-user basis.

The NetScaler URL Threat Intelligence Subscription service provides updates every few minutes to the local cache on the NetScaler SWG appliance. The local cache is based on geolocation to enable quicker action on providing or denying access to sites. If a requested URL is not in the local cache, then the reputation and categorization information will be gathered from the cloud.

The security categories that are considered potential threats and are blocked include illegal activities, illegal drugs, terrorism/extremism, weapons, hate, porn, nudity, sexual services, adult search, hacking, malware, remote proxies, gambling, grotesque, adult magazines/news, advertisements/banners, spam, peer-to-peer, spyware, botnets, infected sites, phishing sites, keyloggers, mobile malware, bot phone home, piracy, and copyright theft.

This service helps maximize employee productivity and reduce security risks by blocking access to millions of malicious sites.

User identity and tailored security policies

NetScaler SWG tracks user identity to network addresses. It helps to enable user-based security policies by tracking users' web activity. Based on bandwidth usage and/or applications accessed, administrators can block or rate-limit the user or group.

Reporting

NetScaler SWG sits in a strategic location for outbound web access, ensuring a natural place to monitor and report on web usage trends. It can log every request or log only those requests that trigger a risk alert.

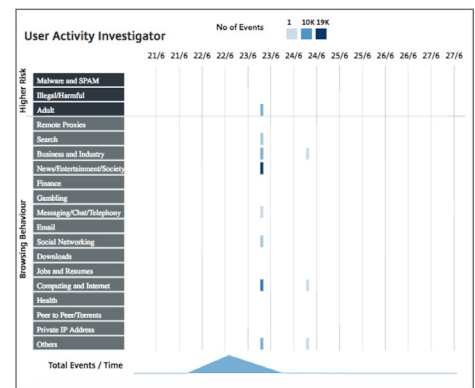
User Behavior Analytics

NetScaler SWG together with NetScaler MAS provides User Behavior Analytics based on user risk score.

Security operations teams gain deep visibility and real-time user behavior analytics to protect against malware threats.

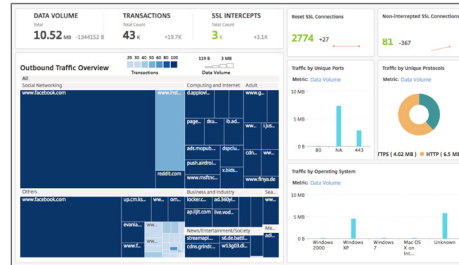
When NetScaler MAS is integrated with the NetScaler SWG appliance, user activity logs and subsequent records on the appliance are exported to NetScaler MAS through a log stream. NetScaler MAS collates and presents user activity information such as websites visited and bandwidth spent. It reports bandwidth usage and any threats detected from malware and phishing sites. The user risk score can be used to quarantine users if they are accessing malicious content.

NetScaler MAS provides two dashboards, the Outbound Traffic Dashboard and the User Dashboard. These dashboards display multiple charts that summarize the websites or applications accessed from the enterprise network and also the activities performed by users in the network.



Outbound Traffic Dashboard

The Outbound Traffic Dashboard provides a summary of the URLs or domains accessed from the enterprise network. It gives a holistic view of all the URLs or domains by number of transactions or data volume consumed.



User Dashboard

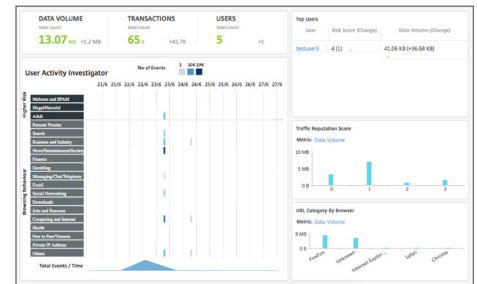
The User Dashboard displays a summary of the activities performed by users in the enterprise. It provides key metrics that can be used to determine:

- Browsing behavior of users in the enterprise
- URL categories accessed by users in the enterprise
- Top five users based on their high-risk scores and bandwidth they consumed
- Browsers used to access the URLs or domains
- Amount of web traffic generated by users, based on the traffic reputation score

The User Dashboard includes a User Activity Investigator pane that displays various web activities performed by users. The pane shows the URL categories accessed by users during a specified time frame and the various events triggered per URL category.

The User Activity Investigator displays key information such as browsing behavior of the user, high-risk activity by the user, and the triggered events per URL category. The events are shown as rectangular legends on a chart. Each of the legends is aggregated at one-minute intervals if the selected duration is one hour, or at one-hour intervals if the selected duration is one day.

Clicking the events brings up the transaction-level details.



User Transactions

The User Transactions page displays the details of user transactions in your network such as:

- Time the transaction occurred
- Protocol used for the transaction
- User name
- Domain that was accessed by the user
- URL category
- Proxy server used to intercept the transaction
- Client port details
- Bytes in and bytes out

Time	Protocol	User	Domain	URL Category	Virtual Server	Client Port	Bytes In	Bytes Out
Jun 24 06:50 AM	HTTP	testuser	al2react.com	Others	trans_cs	NA	80	146
Jun 24 06:50 AM	HTTP	testuser	medaob.kicker.de	Others	trans_cs	NA	240	438
Jun 24 06:50 AM	HTTP	testuser	www.google.com	Others	trans_cs	NA	120	219
Jun 24 06:50 AM	HTTP	testuser	wp3.com	Others	trans_cs	NA	120	219
Jun 24 06:50 AM	HTTP	testuser	www.facebook.com	Others	trans_cs	NA	120	219
Jun 24 06:50 AM	HTTP	testuser	pages2.googleplaydata.com	Others	trans_cs	NA	40	73
Jun 24 06:50 AM	HTTP	testuser	adm.mopub.com	Others	trans_cs	NA	120	219
Jun 24 06:50 AM	HTTP	testuser	frame.alday.de	Others	trans_cs	NA	120	219
Jun 24 06:50 AM	HTTP	testuser	adnfs.largame	Others	trans_cs	NA	120	219
Jun 24 06:50 AM	HTTP	testuser	prabystatic.com	Others	trans_cs	NA	120	219
Jun 24 06:50 AM	HTTP	testuser	lodecon.com	Others	trans_cs	NA	120	219
Jun 24 06:50 AM	HTTP	testuser	wp3.com	Others	trans_cs	NA	40	73
Jun 24 06:50 AM	HTTP	testuser	cms.megaplat	Others	trans_cs	NA	40	73
Jun 24 06:50 AM	HTTP	testuser	medaob.kicker.de	Others	trans_cs	NA	120	219
Jun 24 06:50 AM	HTTP	testuser	ad30qvid.com	Others	trans_cs	NA	120	219

Industry-leading performance

SSL decryption operates at line rate, providing visibility into encrypted traffic without hindering device or network performance. The appliance supports decryption of up to 38 Gbps of SSL traffic for all SSL/TLS versions. With high connection rate/flow count, it can inspect up to 600,000 concurrent SSL sessions and support teardown and setup of up to 80,000+ new SSL transactions per second.

NetScaler Platform	MPX 14040 SWG	MPX 14030 SWG	MPX 14020 SWG
Platform attributes			
Memory	64 GB	64 GB	64 GB
Ethernet ports	16x 10GE SFP+	16x 10GE SFP+	16x 10GE SFP+
Transceivers support	10GE SFP+: SR, LR; 1G cu	10GE SFP+: SR, LR; 1G cu	10GE SFP+: SR, LR; 1G cu
Raid support	Yes	Yes	Yes
Platform performance			
SSL transactions/sec (2k)*	35,000	33,000	25,000
System throughput, Gbps	13	11	7
Concurrent SSL sessions	600,000	600,000	600,000
Platform mechanical, environmental, and regulatory			
Power supplies	2	2	2
Input voltage	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz
Optional DC power supply	Yes	Yes	Yes
Max power consumption	528W	528W	528W
Typical power consumption	300W 1024 BTU/Hr	300W 1024 BTU/Hr	300W 1024 BTU/Hr
Weight, lbs	60	60	60
Height	2U	2U	2U
Width	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets
Depth	28" / 71.2 cm	28" / 71.2 cm	28" / 71.2 cm
Operating temperature	0-40C	0-40C	0-40C
Allowed relative humidity	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing
Safety certifications	CSA	CSA	CSA
Electromagnetic emissions certifications	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
Regulatory compliance	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE
Citrix compliance regulatory model	2U1P1B	2U1P1B	2U1P1B

* Performance varies depending on ciphers deployed. Contact your Citrix sales representative for details.

(Continued on next page)

NetScaler Platform	MPX 14040-40G SWG	MPX 14020-40G SWG
Platform attributes		
Memory	64 GB	64 GB
Ethernet ports (Published Ethernet interfaces compliant per IEEE802.3- 2002/2005/2008/2012)	4x 40GE QSFP+; 16x 10GE SFP+	4x 40GE QSFP+; 16x 10GE SFP+
Transceivers support	40GE QSFP+: SR; 10GE SFP+: SR, LR	40GE QSFP+: SR; 10GE SFP+: SR, LR
Raid support	Yes	Yes
Platform performance		
SSL transactions/sec (2K key certificates)*	35,000	25,000
System throughput, Gbps	13	7
Concurrent SSL sessions	600,000	600,000
Platform mechanical, environmental, and regulatory		
Power supplies	2	2
Input voltage and frequency ranges	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz
Optional DC power supply	Yes	Yes
Max power supply	528W	528W
Typical/max power consumption	300W 1024 BTU/Hr	300W 1024 BTU/Hr
Weight, lbs	60	60
Height	2U	2U
Width	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets
Depth	28" / 71.2 cm	28" / 71.2 cm
Operating temperature	0-40C	0-40C
Allowed relative humidity	5%-95%, non-condensing	5%-95%, non-condensing
Safety certifications	CSA	CSA
Electromagnetic emissions certifica- tions and susceptibility standard	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
Regulatory compliance	RoHS, WEEE	RoHS, WEEE
Citrix compliance regulatory model	2U1P1B	2U1P1B

* Performance varies depending on ciphers deployed. Contact your Citrix sales representative for details.

(Continued on next page)

NetScaler Platform	MPX 14100-40S SWG	MPX 14080-40S SWG	MPX 14060-40S SWG	MPX 14040-40S SWG
Platform attributes				
Memory	64 GB	64 GB	64 GB	64 GB
Ethernet ports (Published Ethernet interfaces compliant per IEEE802.3- 2002/2005/2008/2012)	4x 40GE QSFP+; 8x 10GE SFP+	4x 40GE QSFP+; 8x 10GE SFP+	4x 40GE QSFP+; 8x 10GE SFP+	4x 40GE QSFP+; 8x 10GE SFP+
Transceivers support	40GE QSFP+: SR; 10GE SFP+: SR, LR	40GE QSFP+: SR; 10GE SFP+: SR, LR	40GE QSFP+: SR; 10GE SFP+: SR, LR	40GE QSFP+: SR; 10GE SFP+: SR, LR
Raid support	Yes	Yes	Yes	Yes
Platform performance				
SSL transactions/sec (2K key certificates)*	84,000	82,000	75,000	64,000
System throughput, Gbps	38	34	34	24
Concurrent SSL sessions	600,000	600,000	600,000	600,000
Platform mechanical, environmental, and regulatory				
Power supplies	2	2	2	2
Input voltage and frequency ranges	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz
Optional DC power supply	Yes	Yes	Yes	Yes
Max power supply	528W	528W	528W	528W
Typical/max power consumption	300W 1024 BTU/Hr	300W 1024 BTU/Hr	300W 1024 BTU/Hr	300W 1024 BTU/Hr
Weight, lbs	60	60	60	60
Height	2U	2U	2U	2U
Width	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets
Depth	28" / 71.2 cm	28" / 71.2 cm	28" / 71.2 cm	28" / 71.2 cm
Operating temperature	0-40C	0-40C	0-40C	0-40C
Allowed relative humidity	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing
Safety certifications	CSA	CSA	CSA	CSA
Electromagnetic emissions certifica- tions and susceptibility standard	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
Regulatory compliance	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE
Citrix compliance regulatory model	2U1P1B	2U1P1B	2U1P1B	2U1P1B

* Performance varies depending on ciphers deployed. Contact your Citrix sales representative for details.

(Continued on next page)

	VPX 200 SWG	VPX 1000 SWG	VPX 3000 SWG	VPX 5000 SWG	VPX 8000 SWG
vCPUs ¹	2	2-4	2-4	2-6	2-6
Minimum memory ²	4 GB	4 GB	4 GB	4 GB	4 GB
Performance³					
SSL transactions/sec (2k key certificates)	900	1800	2000	4000	4000
SSL throughput	200 Mbps	1000 Mbps	2.5 Gbps	5 Gbps	5.7 Gbps
Concurrent SSL sessions ⁴	14,000	140,000	150,000	400,000	500,000

1. The minimum number of vCPUs required for a VPX instance is two vCPUs.

2. For NetScaler SWG VPX, the minimum memory requirement is 4 GB for up to two vCPUs. For the optimal performance, we recommend 4 GB memory per vCPU. For example, for a VPX with six vCPUs, we recommend you have 6 x 4 GB = 24 GB memory allocated.

3. Citrix NetScaler performance on VPX appliance on ESXi 6.5, host CPU Intel® Xeon® CPU E5-2690 v4 at 2.60 GHz and 256 GB memory.

4. Concurrent SSL sessions is memory dependent.

Technical aspects

Protects enterprise users and network from internet-bound threats

- Forward proxy for all outbound traffic
- Explicit and transparent proxy
- Visibility into encrypted traffic
- SSL interception bypass policies
- URL Threat Intelligence Subscription
- 170+ URL categories
- 25+ URL category groups
- URL reputation score for all URLs
- URL blacklist/whitelist
- Internet Watch Foundation (IWF) support
- User authentication and authorization
- User identity extraction
- SSL interception error learning mode
- Built-in CA certificate store
- Highly secure cipher support
- TLS 1.2, TLS 1.1, TLS 1.0 support

Simplified management and deployment user interface

- Secure web-based GUI
- Easy-to-use NetScaler SWG wizard
- SSH-based CLI access network management
- SNMP
- Syslog-based logging

Analytics and Reporting

- User Behavior Analytics
- User Risk Score
- Transaction-level view
- Outbound Traffic Dashboard
- User Dashboard
- User Activity Investigator
- User Transactions
- Record export over log stream



Enterprise Sales

North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations

Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States

© 2017 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).