

Security Audit Report

Prepared for: UTM

Delivered on: October 09, 2015

Report Duration: October 08 - October 08, 2015



Security Audit Report

Sophos Firewall was used to conduct a quick network security risk assessment at UTM. This report aims to provide visibility into potential application and web risks, risky users, intrusion risks and usage of applications within UTM network, thereby highlighting security issues that can be addressed by UTM. This report helps organizations understand capabilities of Sophos Firewall to see threats and network usage that their existing firewalls may not see.

Today's dynamic threat landscape requires organizations to re-consider security at their network perimeter every few years. As a result, the Sophos Firewall deployment has begun taking over the mantle of network protection from the last generation of firewalls and security appliances. The truth is, previous generation firewalls are not equipped to identify modern day security threats and do not provide adequate protection, leaving organization networks vulnerable against the tide of new threat vectors and actors.

Sophos Firewall with Layer 8 Identity-based technology offer actionable security intelligence and controls to enterprises, giving complete control over user-level policy enforcement for future-ready security. Sophos Firewall integrates multiple features over a single platform, eliminating the need to manage multiple solutions and hence reduces complexity.

This report provides a high level overview of UTM's network that covers:

- Report Findings
- User Behavior
- User-Application Risks & Usage
- Web Risks & Usage
- Intrusion attacks
- Advanced Threat Protection (ATP)

Report Findings:

Key Observations

■ User-Application Risks and Usage

- UTM faces low Application risk with an App Risk score of 0.41
- 4 risk-prone applications were found traversing the network, of which 1 was very high risk application and 3 were high risk applications.

Key observations on top high risk applications:

Application Category	Number of "Risk-5 & Risk-4" Applications found
P2P	2
General Internet	1
Infrastructure	1

■ Web Risks & Usage

- 1 objectionable web domain was accessed that belonged to Download Freeware & Shareware (1 web domain).
- Top Web categories by data transfer include Content Delivery, Online Shopping, Information Technology.
- Top 45 web domains account for 70% of data transfer due to web surfing.

■ Intrusion attacks

- Overall 903 intrusion attacks with Moderate severity and above were found, including 41 attacks with Major severity and 862 attacks with Moderate severity.
- Top attack categories include Web Services and Applications, Reconnaissance, Operating System and Services, Misc, Browsers.

User Behavior

Studies have proved that users are the weakest link in the security chain and patterns of human behavior can be used to predict and prevent attacks. Also usage pattern can help understand how efficiently are corporate resources utilized and if user policies need to be fine-tuned.

The Layer 8 Technology over Sophos Firewalls treat user identity as the 8th layer or the "human layer" in the network protocol stack. This allows administrators to uniquely identify users, control Internet activity of these users in the network, and enable policy-setting and reporting by username.

Users with risk-prone behavior

User Threat Quotient (UTQ) helps security administrators spot users posing risk, based on suspicious web behavior and advanced attacks triggered from their hosts. The risk could be a result of unintended actions due to lack of security awareness or malware infected host or intended actions of a rogue user. Knowing the user and the activities that caused risk can help the Network Security administrator take required actions to avoid such risks.

Users with risk-prone behavior

Relative Risk Ranking	User	Relative Threat Score
No Record Found.		

User Application Risks & Usage

Today, it is crucial for an organization to be aware about the applications traversing the network and potential risks they pose in order to effectively manage related business risks. Sophos Firewall Application Visibility & Control offers complete visibility on which applications are being accessed within the network irrespective of their ports and protocols. This stops sophisticated application-layer threats right at the network perimeter.

Application Risk Score

This risk calculator indicates the overall risk associated with various applications and is calculated on the basis of individual risk associated with a specific the application and number of hits on that application.

Risk: 0.41

High Risk Applications in use

The table below lists top 4 high risk applications (risk rating 5 or 4 in this order) along with risk level, application category, characteristic and technology to help understand potential application high risks faced by the network.

High risk applications

Risk Level	App Name	Category	Technology	Hits	Bytes
5	Torrent Clients P2P	P2P	P2P	131	185.95 KB
4	HTTP	General Internet	Browser Based	323	65.36 MB
4	FTP Base	Infrastructure	Client Server	1	7.31 KB
4	QQ Download P2P	P2P	Client Server	1	116 B

Application Categories & Applications

Knowing top app categories and applications help understand how efficiently are corporate resources utilized and also app filtering policies. These reports provide a snapshot of various application categories and applications accessed by users and amount of Internet traffic generated by them.

Application Categories by Data Transfer

Application Category	Hits	Bytes
Infrastructure	7804	1.29 GB
Streaming Media	110	573.67 MB
General Internet	801	73.36 MB
N/A	21943	15.81 MB
Software Update	41	10.9 MB
Remote Access	1	9.27 MB
File Transfer	398	2.4 MB
Mobile Applications	122	1.33 MB
P2P	132	186.06 KB
Web Mail	7	158.99 KB
Network Services	6	70.05 KB
General Business	1	7.81 KB

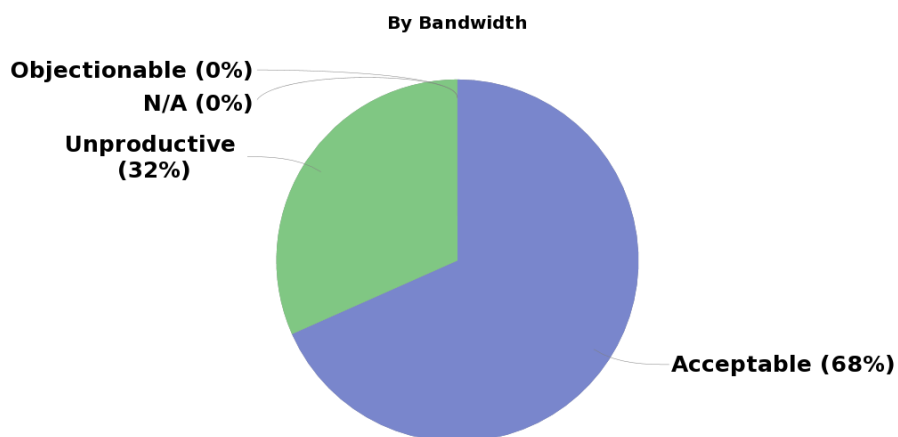
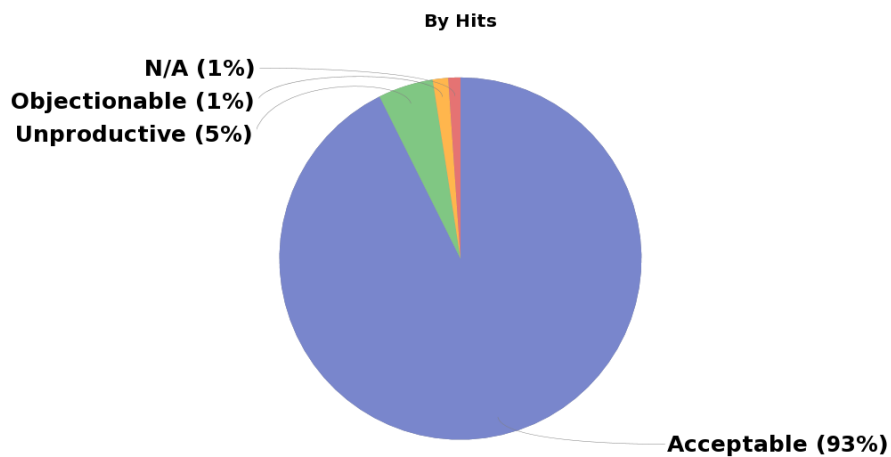
Top 20 Applications by Data Transfer

Application	Application Risk	Application Category	Hits	Bytes
NetBIOS	1	Infrastructure	1951	1.26 GB
iTunes Internet	3	Streaming Media	101	573.67 MB
HTTP	4	General Internet	323	65.36 MB
Secure Socket Layer Protocol	1	Infrastructure	3977	30.36 MB
Windows Remote Desktop	3	Remote Access	1	9.27 MB
Apple Appstore	3	General Internet	470	7.98 MB
MS Essentials AV Update	3	Software Update	2	7.77 MB
UDP:514	N/A	N/A	800	5.06 MB
TCP:443	N/A	N/A	1099	4.16 MB
UDP:161	N/A	N/A	14648	3.74 MB
Apt-Get Command	2	Software Update	10	2.52 MB
iCloud	3	File Transfer	398	2.4 MB
TCP:54390	N/A	N/A	1	1.16 MB
UDP:1900	N/A	N/A	399	590.52 KB
Microsoft Updates	1	Software Update	25	587.31 KB
iCloud Contacts	1	Mobile Applications	45	574.19 KB
DNS	1	Infrastructure	1699	562.46 KB
iCloud Bookmarks	1	Mobile Applications	51	445.17 KB
UDP:3544	N/A	N/A	1881	410.39 KB
BITS	2	Infrastructure	3	313.09 KB

Web Risks & Usage Visibility

Organizations need a strong security mechanism, which is capable to block access to harmful websites, prevent malware, phishing, pharming attacks and undesirable content that could lead to legal liability & direct financial losses. Being able to do so also enables them to manage productivity of their users and helps achieve effective utilization of bandwidth.

Sophos Firewall Web Filtering offers one of the most comprehensive URL databases with millions of URLs providing Web Security, HTTPS Controls and comprehensive Web & Content filtering solution.



Objectionable Web Categories & Domains being accessed

These reports help administrator monitor objectionable web categories and domains.

Objectionable Web Categories

Category	No of domains	Bytes	Hits
Download Freeware & Shareware	1	14.02 KB	9

Objectionable web domains

Web Domains	Web Category	Bytes	Hits
sr.symcd.com	Download Freeware & Shareware	14.02 KB	9

Web Categories & Domains

These reports offer insights into the user's browsing habits that can help understand how efficiently corporate resources get utilized and efficacy of web filtering policies.

This Report displays a list of top web categories along with the number of hits.

Web categories by Hits

Category	Bytes	Hits
IPAddress	724.03 KB	277
Information Technology	70.2 MB	240
Content Delivery	347.53 MB	81
Online Shopping	193.75 MB	28
Download Freeware & Shareware	14.02 KB	9
InvalidUrl	16.05 KB	6
Portal Sites	2.08 KB	4
Uncategorized	2 B	2
Search Engines	231 B	1
General Business	1.64 KB	1
None	6.56 KB	1
CRL and OCSP	3.35 KB	1

Web categories by Data Transfer

Category	Hits	Bytes
Content Delivery	81	347.53 MB
Online Shopping	28	193.75 MB
Information Technology	240	70.2 MB
IPAddress	277	724.03 KB
InvalidUrl	6	16.05 KB
Download Freeware & Shareware	9	14.02 KB
None	1	6.56 KB
CRL and OCSP	1	3.35 KB
Portal Sites	4	2.08 KB
General Business	1	1.64 KB
Search Engines	1	231 B
Uncategorized	2	2 B

Top 15 Web Domains by Hits

Web Domain	Web Category	Bytes	Hits
192.168.0.200:10000	IPAddress	103.15 KB	125
peerserver3-ncal.netgear.com	Information Technology	149 B	100
192.168.0.105	IPAddress	559.97 KB	91
peerserver2-ncal.netgear.com	Information Technology	72 B	72
192.168.0.201:10000	IPAddress	43.74 KB	53
apt.readynas.com	Information Technology	1.62 MB	28
mirrors.kernel.org	Information Technology	933 B	15
is1.mzstatic.com	Content Delivery	29.54 KB	11
sr.symcd.com	Download Freeware & Shareware	14.02 KB	9
security.debian.org	Information Technology	101.44 KB	7
is2.mzstatic.com	Content Delivery	26.39 KB	7
update.readynas.com	Information Technology	60.46 MB	7
fastvue	InvalidUrl	16.05 KB	6
192.168.0.100:5357	IPAddress	12.87 KB	6
is3.mzstatic.com	Content Delivery	14.43 KB	5

Top 15 Web Domains by Data Transfer

Web Domain	Web Category	Hits	Bytes
update.readynas.com	Information Technology	7	60.46 MB
a409.phobos.apple.com	Content Delivery	1	12.33 MB
a1438.phobos.apple.com	Online Shopping	1	9.84 MB
a1782.phobos.apple.com	Content Delivery	1	9.74 MB
a1458.phobos.apple.com	Online Shopping	1	9.63 MB
a464.phobos.apple.com	Online Shopping	1	9.6 MB
a596.phobos.apple.com	Content Delivery	2	9.54 MB
a1322.phobos.apple.com	Content Delivery	1	9.43 MB
a502.phobos.apple.com	Content Delivery	1	9.36 MB
a1510.phobos.apple.com	Content Delivery	1	9.33 MB
a1167.phobos.apple.com	Content Delivery	1	9.14 MB
a271.phobos.apple.com	Content Delivery	1	9.13 MB
a1127.phobos.apple.com	Content Delivery	1	9.06 MB
a1216.phobos.apple.com	Content Delivery	1	8.86 MB
a1105.phobos.apple.com	Content Delivery	1	8.82 MB

Intrusion Attacks

Detection and protection against network and application level attacks like intrusion attacks, malicious code transmission, backdoor activity is critical to protect network from hackers. Sophos Firewall's Intrusion Prevention System helps strengthen defenses against network-level and application-level attacks.

Number of attacks by Severity-level

	Major	Minor	Moderate	Warning
Total attacks	41	870	862	53

Intrusion Attacks

This Report fetches details for the top attacks that have hit the system with information of their severity level, category, platform, target and attack count.

Intrusion attacks by Severity

Severity-level	Attack	Category	Platform	Target	Attack Count
Major	HP Intelligent Management Center imcsyslogdm Use After Free	Application and Software	Linux,Windows	Server	41
Minor	SCAN UPnP service discover attempt	Reconnaissance	BSD,Linux,Mac,Other,Solaris,Unix,Windows	Server	870
Moderate	(snort_decoder) WARNING: MISC IP option set	N/A	N/A	N/A	597
Moderate	SSL Request Export Ciphersuite Detection	Browsers	BSD,Linux,Mac,Solaris,Unix,Windows	Client,Server	155
Moderate	(snort_decoder) WARNING: IPV4 packet to broadcast dest address	N/A	N/A	N/A	71
Moderate	SSLv3.0 ClientHello from vulnerable client - CVE-2014-3566	Operating System and Services	BSD,Linux,Mac,Solaris,Unix,Windows	Client,Server	20
Moderate	OpenSSL ClientHello signature_algorithm Extension Denial of Service	Operating System and Services	Other	Client	10
Moderate	HTTPS/SSL Renegotiation DoS	Web Services and Applications	BSD,Linux,Mac,Other,Solaris,Unix,Windows	Server	5
Moderate	(snort_decoder) WARNING: IPV4 packet from 'current net' source address	Reconnaissance	BSD,Linux,Mac,Other,Solaris,Unix,Windows	Server	2
Moderate	SHELLCODE x86 setuid 0	Misc	BSD,Linux,Mac,Other,Solaris,Unix,Windows	Client,Server	2
Warning	ICMP Destination Unreachable Host Unreachable	Reconnaissance	BSD,Linux,Mac,Other,Solaris,Unix,Windows	Server	33

Severity-level	Attack	Category	Platform	Target	Attack Count
Warning	ICMP PING	Reconnaissance	BSD, Linux, Mac, Other, Solaris, Unix, Windows	Server	10
Warning	ICMP Echo Reply	Reconnaissance	BSD, Linux, Mac, Other, Solaris, Unix, Windows	Server	10

Attack categories

Attack Category	Variety of attacks	Attack Count
Reconnaissance	5	925
N/A	2	668
Browsers	1	155
Application and Software	1	41
Operating System and Services	2	30
Web Services and Applications	1	5
Misc	1	2

Advanced Threat Protection (ATP)

Made simple to use, Sophos Advanced Threat Protection protects enterprise networks from falling prey to botnet risks and helps identify infected endpoints, so the administrator can take immediate action.

Summary

Threat Count	Host Count	Events
0	0	N/A

Advanced Threats

Threat	Host Count	Origin	Events
No Record Found.			

Hosts - ATP

Host (Source IP)	Threat count	Events
No Record Found.		

Detailed View - ATP

Host (Source IP)	User	Threat	Threat URL/IP	Origin	Events	Action
No Record Found.						