

360-Degree Security Review

Report Date: July 31, 2018 11:16

Data Range: 2018-07-24 00:00 2018-07-30 23:59 CST (FAZ local)

Table of Contents

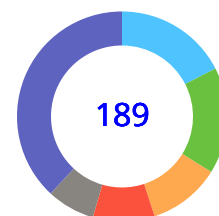
Summary	2
1. Application Visibility and Control	3
High Risk Applications in Use	3
High Risk Application by Category	4
Application Risk Definition	5
Application Categories	6
Web Application	7
Web Categories	8
2. Threat Detection and Prevention	9
Malware: Viruses, Bots, Spyware/Adware, Phishing Sites	9
Intrusion and Attacks	13
Advanced Threats	14
3. Data Exfiltration Detection and Prevention	15
4. Endpoint Detection and Prevention	16
5. Recommended Actions	18
Appendix A	19
Devices	19

Summary

This report provides the findings of the comprehensive security review that Fortinet conducted for your network. Fortinet next generation firewall FortiGate 1500D is used for this analysis. This report begins with a summary of these findings, followed by details of the threats, applications and type of content found and closes with a set of recommended actions.

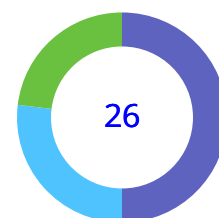
Application Visibility and Control

General.Interest	33
Collaboration	31
Network.Service	21
Video/Audio	18
Social.Media	14
Others	72



Threat Detection and Prevention

Malicious & Phishing Sites	13
Critical & High Intrusion Attack	7
Malware & Botnet C&C	6



Data Exfiltration Detection and Prevention

No matching log data for this report

Endpoint Protection

No matching log data for this report

1. Application Visibility and Control

The following sections provide findings on high risk applications identified on your network. It has been determined by FortiGuard Lab that these applications represent possible vectors for data compromise, network intrusion, or a reduction in network performance.

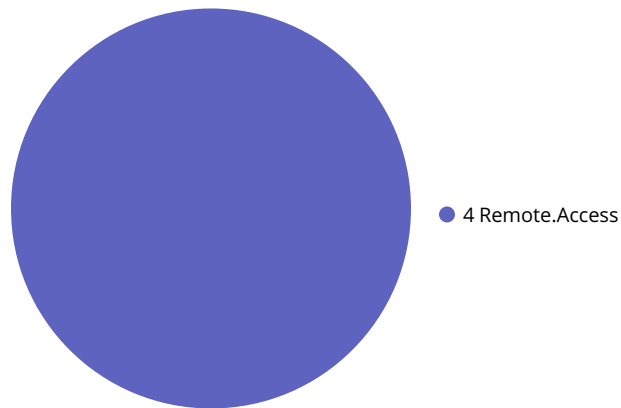
High Risk Applications in Use

Top 20 high risk applications are listed below. These applications have the risk rating of 5(severe risk) or 4(high risk). Each application is listed with its respective category, technology, number of users, total bytes and sessions.

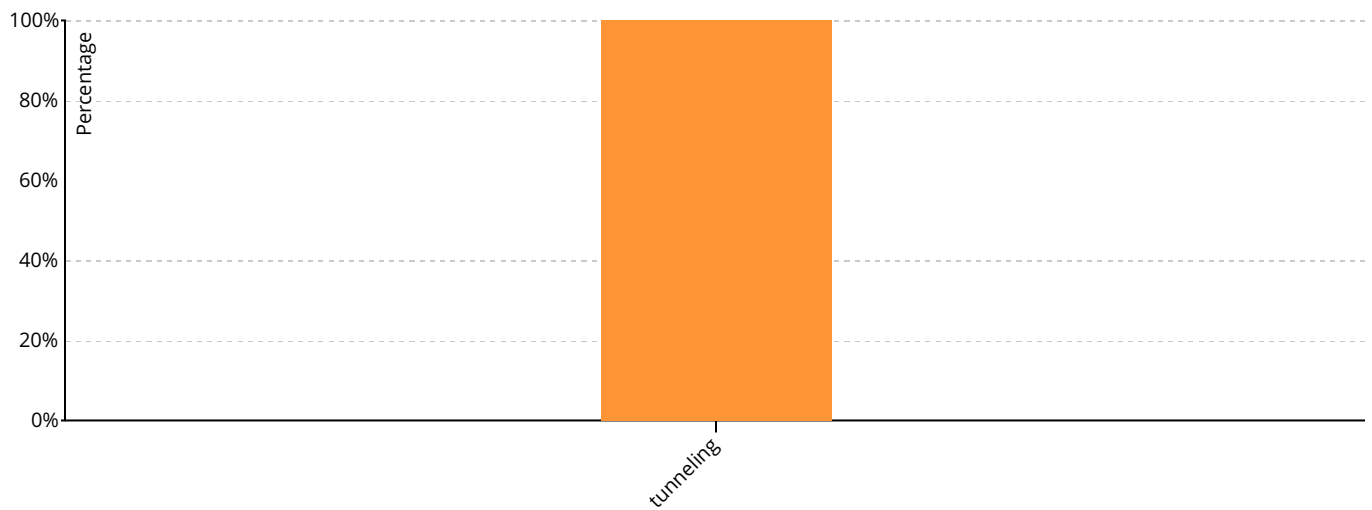
Risk	Application Name	Category	Technology	User	Total Bytes	Session
4	AnyDesk	Remote.Access	Client-Server	7	40.05 MB	115
4	TeamViewer	Remote.Access	Client-Server	8	1.63 MB	68
4	Citrix.Receiver	Remote.Access	Client-Server	2	106.38 KB	3
4	TeamViewer_CallRequest	Remote.Access	Client-Server	2	1.28 MB	2

High Risk Application by Category

Breakdown of the high risk applications by application category



Behavioural characteristics of the high risk applications



Application Risk Definition

The FortiGuard research team assigns a risk rating of 1 to 5 to an application based on the application behavioural characteristics. The risk rating can help administrators to identify the high risk applications quickly and make a better decision on the application control policy.

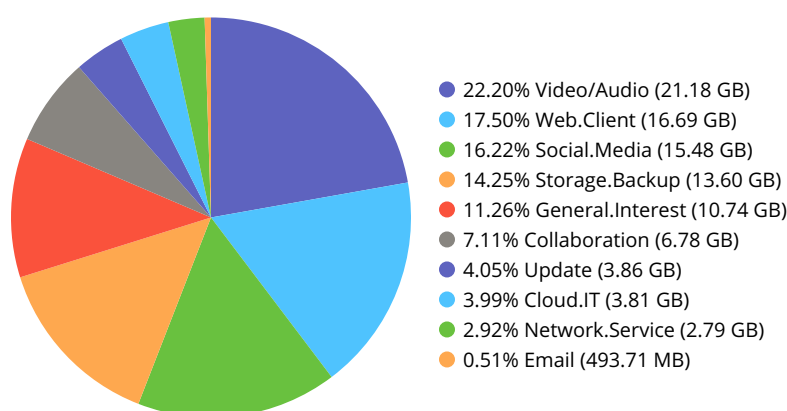
Risk Rating	Behavior Characteristics	Examples
5 Severe	Malicious applications or the applications that can bypass security	Botnet or Proxy applications
4 High	Applications that can cause malware infection or data leakage: often these applications are used for personal file-sharing or tunnelling other applications	P2P or Remote.Access applications
3 Elevated	Applications are used for personal communication or have known vulnerabilities	IM,Email,Storage.Backup applications
2 Guarded	Applications consume bandwidth or affect productivity	Game,Social.Media,Video/Audio applications
1 Low	Business applications or software update applications	Update or Business applications

Application Categories

The FortiGuard research team categorized applications into different categories based on the application behavioural characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application management. For application category details, see: <http://www.fortiguard.com/encyclopedia/applications>.

The following section shows the application category breakdown of all the applications on the network, sorted by bandwidth. This information helps network administrator to identify where the bandwidth is used, and how many applications use it. Armed with this information, the administrators can effectively prioritize the applications based on the business needs: for example, allow business applications but traffic shape the applications for personal use.

Top 10 application categories by bandwidth usage



Category breakdown of all applications, sorted by bandwidth usage

Category	Number of Applications	User	Total Bytes	Session
Video/Audio	18	48	21.18 GB	18,782
Web.Client	9	73	16.69 GB	174,333
Social.Media	14	60	15.48 GB	30,245
Storage.Backup	11	43	13.60 GB	24,213
General.Interest	33	68	10.74 GB	93,203
Collaboration	31	60	6.78 GB	119,069
Update	10	43	3.86 GB	12,891
Cloud.IT	7	43	3.81 GB	8,719
Network.Service	20	65	2.79 GB	105,518
Email	10	43	493.71 MB	5,601
Business	11	50	69.93 MB	3,365
Remote.Access	4	13	43.06 MB	188
Mobile	2	8	29.41 MB	617
Unknown	156	42	27.17 MB	19,211
Proxy	1	2	23.77 MB	5
Game	4	7	550.03 KB	1,583
VoIP	3	7	321.62 KB	102

Web Application

Web applications allow users to submit and retrieve content over the internet and they pose a great security risk to the business. Sensitive customer data or confidential business trade secrets can be leaked by employees using vulnerable web applications; applications that can be exploited by attackers using code injection to trick users and redirect them towards.

The following section shows the top 25 web applications with their application risk ratings, sorted by bandwidth usage.

Risk	Application Name	Category	Technology	User	Total Bytes	Session
2	YouTube	Video/Audio	Browser-Based	46	17.30 GB	11,356
3	HTTPS.BROWSER	Web.Client	Browser-Based	69	14.50 GB	151,949
3	iCloud	Storage.Backup	Browser-Based,Client-Serv er	24	12.26 GB	20,140
3	Facebook	Social.Media	Browser-Based	57	5.82 GB	19,960
2	Facebook_Video.Play	Social.Media	Browser-Based	29	5.73 GB	1,698
2	MS.Windows.Update	Update	Client-Server	31	3.59 GB	8,632
3	Amazon.AWS_S3	Cloud.IT	Browser-Based	28	3.39 GB	1,605
2	Tumblr	Social.Media	Browser-Based	2	3.21 GB	423
2	Google.Services	General.Interest	Browser-Based	62	3.11 GB	34,718
2	Netflix	Video/Audio	Browser-Based	11	2.98 GB	422
2	WhatsApp_File.Transfer	Collaboration	Client-Server	33	2.28 GB	1,210
2	Apple.Store	General.Interest	Client-Server	24	1.80 GB	2,406
2	HTTP.Segmented.Downloa d	Network.Service	Browser-Based	27	1.61 GB	276
2	Amazon.Services	General.Interest	Browser-Based	24	1.42 GB	4,078
2	Microsoft.CDN	Collaboration	Browser-Based	35	1.25 GB	6,186
2	WhatsApp_Web	Collaboration	Browser-Based	31	1.21 GB	5,153
3	HTTP.BROWSER	Web.Client	Browser-Based	62	1.20 GB	7,294
3	Apple.iCloud.Storage	Storage.Backup	Client-Server	4	1.15 GB	136
2	Google.Accounts	General.Interest	Browser-Based	56	725.70 MB	13,379
2	Microsoft.Portal	Collaboration	Browser-Based	42	584.83 MB	26,061
2	HTTP.BROWSER_Chrome	Web.Client	Browser-Based	37	489.71 MB	5,920
2	Twitter	Social.Media	Browser-Based	39	486.35 MB	3,906
3	Spotify	Video/Audio	Client-Server	17	447.24 MB	6,337
2	WebEx	Collaboration	Browser-Based,Client-Serv er	17	408.43 MB	1,217
3	Gmail	Email	Browser-Based	35	326.56 MB	3,701

Web Categories

Identifying which web categories and websites are accessed by applications provides additional data points for administrators to understand the network traffic usage. Defining appropriate application policies along with web filtering policies will greatly reduce the business risk.

Fortinet's proprietary web filtering database is developed by the FortiGuard research team. The database contains more than 47 million rated websites with real-time updates; the websites are categorized into 76 web categories to allow highly-granular web filtering policies. For web filter categories see: <http://www.fortiguard.com/static/webfiltering.html>

The following section shows the most commonly visited web categories with their respective bandwidth usage.

Webfilter URL	User	Count	Total Bytes
Information Technology	54	102,125	15.16 GB
Search Engines and Portals	51	31,395	3.01 GB
Advertising	49	25,679	774.73 MB
Content Servers	50	15,717	3.17 GB
Social Networking	47	15,286	8.26 GB
Internet Telephony	40	13,461	321.33 MB
Business	41	11,844	455.04 MB
Freeware and Software Downloads	35	11,607	77.26 MB
Internet Radio and TV	31	11,197	412.18 MB
File Sharing and Storage	42	8,595	495.85 MB
Streaming Media and Download	43	5,324	13.94 GB
Web Analytics	35	4,073	35.45 MB
Web Chat	27	3,848	558.28 MB
Shopping	32	3,574	734.85 MB
Instant Messaging	47	2,973	2.52 GB
Web-based Email	37	2,811	317.94 MB
Unrated	18	2,083	39.03 MB
Auction	11	1,990	129.96 MB
Finance and Banking	23	1,990	156.37 MB
News and Media	29	1,561	91.20 MB
Meaningless Content	37	1,561	88.14 MB
Web-based Applications	31	1,209	194.64 MB
Games	25	1,090	3.96 MB
Travel	14	859	109.93 MB
Online Meeting	16	750	208.17 MB

2. Threat Detection and Prevention







The rise of modern malware has reshaped the threat landscape. These modern threats bypass traditional anti-malware strategies and establish a foothold within the enterprise. They are used by criminals and nation-states to steal sensitive information and attack assets.

Fortinet next generation firewall provides multi-level protection to combat these advanced persistent threat - the reliable visibility and control of all traffic on the network regardless of evasive tactic. The FortiGuard AntiVirus Service employs advanced virus, spyware, and heuristic detection engines to enable FortiGate systems to detect and prevent both new and evolving threats. For AntiVirus see: <http://www.fortiguard.com/antivirus/>

Malware: Viruses, Bots, Spyware/Adware, Phishing Sites

The table below show the common viruses discovered, the botnet C&C communications detected and the spyware/adware and phishing sites found.

Top 10 Malware, Virus or Spayware

Malware Name	Malware Type	Victim	Source	Count
 Malicious_Behavior.SB	Virus	1	2	23
 VBA/TrojanDownloader.JMR!tr	Virus	1	4	6
 Malware_Generic.P0	Virus	1	1	1
 W32/FareitVB.CGGL!tr	Virus	1	1	1
 W32/GenKryptik.CGHM!tr	Virus	1	1	1
 W32/VBKryptik.DZLN!tr	Virus	1	1	1

Top 10 Malware Botnet

No matching log data for this report

Top 10 Botnet C&C Domains and IPs Detected by DNS Filtering

No matching log data for this report


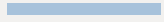

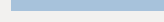
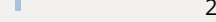
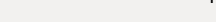


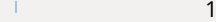
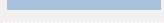
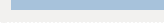
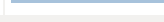
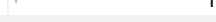



Top 10 Victims of Malware

User(or IP)	Malware	Count	% of Subtotal
80.211.46.224	Malicious_Behavior.SB	21	100.00%
	Subtotal	21	63.64%
192.190.42.62	Malicious_Behavior.SB	2	66.67%
	W32/FareitVB.CGGL!tr	1	33.33%
	Subtotal	3	9.09%
95.211.151.57	VBA/TrojanDownloader.JMR!tr	3	100.00%
	Subtotal	3	9.09%
103.250.184.30	W32/GenKryptik.CGHM!tr	1	100.00%
	Subtotal	1	3.03%
185.82.203.158	VBA/TrojanDownloader.JMR!tr	1	100.00%
	Subtotal	1	3.03%
191.101.26.140	VBA/TrojanDownloader.JMR!tr	1	100.00%
	Subtotal	1	3.03%
196.46.182.42	W32/VBKryptik.DZLN!tr	1	100.00%
	Subtotal	1	3.03%
219.83.54.102	Malware_Generic.P0	1	100.00%
	Subtotal	1	3.03%
50.76.89.49	VBA/TrojanDownloader.JMR!tr	1	100.00%
	Subtotal	1	3.03%
Total		33	100.00%

Top 10 Victims of Phishing Site

User(or IP)	Phishing Site	Count	% of Subtotal
192.168.26.52	https://vault.nqintelligence.com/	45	100.00 %
	Subtotal	45	72.58%
192.168.0.170	http://lifemiles-aliados.massdev.co/wp-content/uploads/2017/08/map-pointer.png	2	50.00%
	http://cumboandrea.me/como-poner-contrasena-a-una-carpeta/	1	25.00%
	http://cumboandrea.me/favicon.ico	1	25.00%
	Subtotal	4	6.45%
192.168.26.63	http://cobalten.com/apu.php?zoneid=1333060	1	33.33%
	http://zukxd6fkxqn.com/1333061.css	1	33.33%
	http://zukxd6fkxqn.com/libs/underscore/0.33.31/underscore.min.js	1	33.33%
	Subtotal	3	4.84%
pablo	https://luj.sdsjweb.com/	2	66.67%
	http://parkingcrew.net/assets/scripts/js3.js	1	33.33%
	Subtotal	3	4.84%
192.168.26.95	https://km.support.apple.com.edgekey.net/	2	100.00 %
	Subtotal	2	3.23%
192.168.26.101	http://app.smokyashan.com/1b0ace0dc6ead67cb1fa595ab1051ff6	1	100.00 %
	Subtotal	1	1.61%
192.168.26.69	http://megapornpics.com/wp-content/uploads/2018/03/porno_occidente_-22939.jpg	1	100.00 %
	Subtotal	1	1.61%
192.168.26.80	http://ads.avocet.io/getuid?url=//x.bidswitch.net/sync?dsp_id%3D59%26user_id%3D%7B%7BUUID%7D%7D%26ssp%3Dpulsepoint%26bsw_param%3Da2f70de9-22fb-47e4-8118-c17c7bfd60aa	1	100.00 %
	Subtotal	1	1.61%
192.168.26.90	http://popcorntime-update.xyz/?app_id=T4PSEC&hid=e88633852a284fc70bac9fa512f177de&ver=5.7.2.0&os=WIN060200	1	100.00 %
	Subtotal	1	1.61%
192.168.75.51	https://c.adsc0.re/	1	100.00 %
	Subtotal	1	1.61%
Total		62	100.00 %

Top 25 Malicious Phishing Sites

Phishing Site	Victims	Source	Count
https://vault.nqintelligence.com/		1 	1 
http://lifemiles-aliados.massdev.co/wp-content/uploads/2017/08/map-point er.png		1 	2 
https://km.support.apple.com.edgekey.net/		1 	2 
https://luj.sdsjweb.com/		1 	2 
http://cumboandrea.me/favicon.ico		1 	1 
http://megapornpics.com/wp-content/uploads/2018/03/porno_occidente_-2 2939.jpg		1 	1 
http://ads.avocet.io/getuid?url=//x.bidswitch.net/sync?dsp_id%3D59%26user _id%3D%7B%7BUUID%7D%7D%26ssp%3Dpulsepoint%26bsw_param%3Da2f 70de9-22fb-47e4-8118-c17c7bfd60aa		1 	1 
http://popcorntime-update.xyz/?app_id=T4PSEC&hid=e88633852a284fc70ba c9fa512f177de&ver=5.7.2.0&os=WIN060200		1 	1 
http://zukxd6fkxqn.com/1333061.css		1 	1 
http://zukxd6fkxqn.com/libs/underscore/0.33.31/underscore.min.js		1 	1 
https://c.adsco.re/		1 	1 
http://parkingcrew.net/assets/scripts/js3.js		1 	1 
http://app.smokyashan.com/1b0ace0dc6ead67cb1fa595ab1051ff6		1 	1 
http://cobalten.com/apu.php?zoneid=1333060		1 	1 
http://cumboandrea.me/como-poner-contrasena-a-una-carpeta/		1 	1 










Intrusion and Attacks

An application vulnerability could be exploited to compromise the security of the network. Once an application vulnerability has been found, the attacker can exploit it to facilitate a cyber crime. The visibility into application vulnerability exploits enables the administrator to take immediate action against a threat and to protect business assets.

The FortiGuard Intrusion Prevention Service(IPS) provides Fortinet customers with the latest defences against stealthy network-level threats. It uses a customizable database of more than 5,100 known threats to stop attacks that evade traditional firewall systems. It also provides behaviour based heuristics analysis to enable the FortiGate systems to recognize zero-day attacks. For application Vulnerability and IPS see:

<http://www.fortiguards.com/static/intrusionprevention.html>

The section below shows application vulnerabilities discovered on the network, ranked by severity and count.

Severity	Malware Name	Malware Type	CVE-ID	Victim	Source	Count
5	 D-Link.DSL-2750B.CLI.OS.Command.Injection	OS Command Injection		2	31	35
5	 MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	Buffer Errors	CVE-2017-7269	2	16	18
5	 Dasan.GPON.Remote.Code.Execution	OS Command Injection	CVE-2018-10561,CVE-2018-10562	2	13	13
5	 Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	Code Injection	CVE-2017-3506,CVE-2017-10271	1	2	2
4	 JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution	OS Command Injection		2	37	38
4	 PHP.CGI.Argument.Injection	Code Injection	CVE-2012-1823,CVE-2012-2311	2	1	2
4	 Obfuscated.Rich.Text.Format	Anomaly	CVE-2018-0802	2	1	2
2	 ZmEu.Vulnerability.Scanner	Malware		1	1	6
2	 Masscan.Scanner	Anomaly		2	1	2

Advanced Threats

A zero-day vulnerability is a previously unknown threat that does not yet have a patch available from the vendor. Commonly used applications such as web browsers and e-mail client applications are often targeted for the zero-day exploits because of their widespread distribution and usage; for example, attacks can send a zero-day malware as e-mail attachments which exploit vulnerabilities in the application opening the attachment.

FortiGuard research team proactively monitors threat landscape and looks for zero-day vulnerabilities; once a zero-day vulnerability is identified, an advanced signature(s) is developed and pushed out to the customers before a vendor's patch release is available. These signatures are unique to Fortinet and play an critical role in the fight against advanced persistent threats(APTs).

The section below provides a summary of the files analyzed by FortiCloud Sandbox during the last period.

No matching log data for this report

The list below provides some examples of the malicious files detected by FortiCloud Sandbox.

No matching log data for this report

Zero-day malware detected on the network by the on-box AntiVirus scanning, sorted by count.

No matching log data for this report

3. Data Exfiltration Detection and Prevention

Applications that have ability to transfer files can pose a significant risk of data loss: company's customer data, intellectual property and confidential business trade secrets can be sent out of the organization via these applications. Knowing which types of files and content are transferred crossing the network can help administrators to mitigate the risk by setting up appropriate application policies along with data leak prevention rules on the Fortinet next generation firewall system.

Data loss incidents summary by severity

No matching log data for this report

The section below lists the most common files and file types along with the service type.

No matching log data for this report

4. Endpoint Detection and Prevention

FortiClient protects your endpoints with an extra layer of security; it's engineered to defeat the latest and most dangerous malware and provides real-time protection on the company's desktops and mobile devices. FortiClient together with Fortinet next generation Firewall delivers fully managed and layered security defences.

Security Events Summary

No matching log data for this report

Endpoints Running High Risk Applications

No matching log data for this report

Endpoints Infected with Malware

No matching log data for this report

Top Endpoints with Web Violations

No matching log data for this report

Top Endpoints with Data Loss Incidents

No matching log data for this report

5. Recommended Actions

Botnet and Malware Infections 6

Bots can be used for launching denial-of-service(Dos) attacks, distributing spam, spyware and adware, propagating malicious code, and harvesting confidential information which can lead to serious financial and legal consequences. Botnet infections need to be taken seriously and immediate action is required. Identify botnet infected computers and clean-up the computers using AntiVirus software. Fortinet AntiVirus product FortiClient can be used to scan the infected computers and remove botnets from the computer.

Evasive Applications 1

Proxy applications are often used to conceal their activity and bypass the security control. This represents both business and security risks to your organization. Implement the application policies to dictate the use of these applications.

P2P Applications 0

These applications can be used to bypass existing content controls and lead to unauthorized data transfer and data policy violations. Policies on appropriate use of these applications need to be implemented.

Bandwidth Consuming Applications 36

Applying application policies to regain control in the use of these applications. One of the options would be a traffic shaping rule to limit consumption.

Deploy a Fortinet Next Generation Firewall

Fortinet next-generation firewalls enable organizations to gain visibility on all application traffic and deliver scalable and secure application control for enterprises. Deploying a Fortinet firewall in your organization and creating secure application policies to ensure that your network is being used according to the organization's priorities.

Appendix A

Devices

Teco