Network Security Services

Menu

1.1 Cybersecurity Assessments

Cybersecurity assessments are crucial for gaining insights into your network vulnerabilities. Here are some details on how to conduct them:

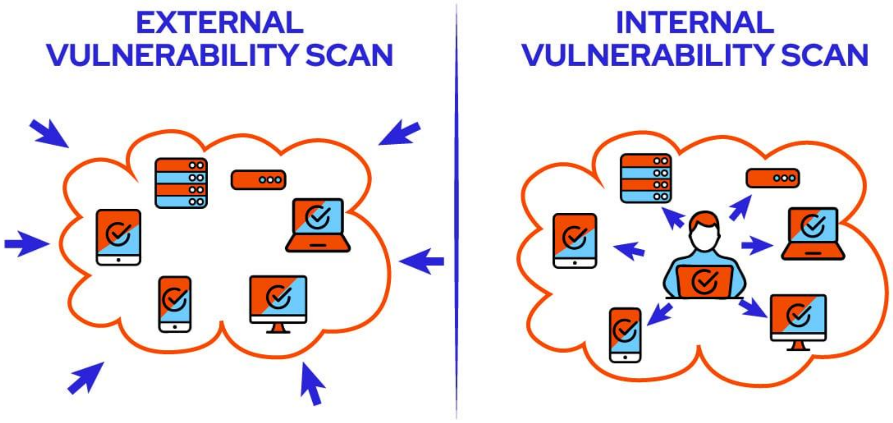
- **Vulnerability Scanning: Use automated tools to scan your network for known vulnerabilities in software, configurations, and systems.**

1. External Vulnerability Scans

- These scans target the areas of your IT ecosystem that are exposed to the internet or are otherwise not restricted to your internal users or systems. They can include websites, ports, services, networks, systems, and applications that need to be accessed by external users or customers.

2. Internal Vulnerability Scans

- These scan and target your internal corporate network. They can identify vulnerabilities that leave you susceptible to damage once a cyberattack or piece of malware makes it to the inside. These scans allow you to harden and protect applications and systems that are not typically exposed by external scans.



3. Environmental Scans

- These scans are based on the environment that your technology operates in. Specialized scans are available for multiple different technology deployments, including cloud-based, IoT devices, mobile devices, websites, and more.

4. Intrusive Versus Non-Intrusive Scans

- Non-intrusive scans simply identify a vulnerability and report on it so you can fix it. Intrusive scans attempt to exploit a vulnerability when it is found. This can highlight the likely risk and impact of a vulnerability, but may also disrupt your operational systems and processes, and cause issues for your employees and customers — so use intrusive scanning with caution.

- **Penetration Testing: Simulate real-world attacks to identify potential entry points for hackers and test the effectiveness of your security measures.**

1. **Planning**

- Ethical hackers discuss the scope and overall goals of the test with key stakeholders. Test methods and success measures are defined during this initial discussion phase. After the basic profile is established, the hacker begins to investigate all the components of the corporate network.

2. **Testing**

- Ethical Hackers use static or dynamic testing solutions to study and understand how networks respond to simulated attacks.

3. **Accessing Network**

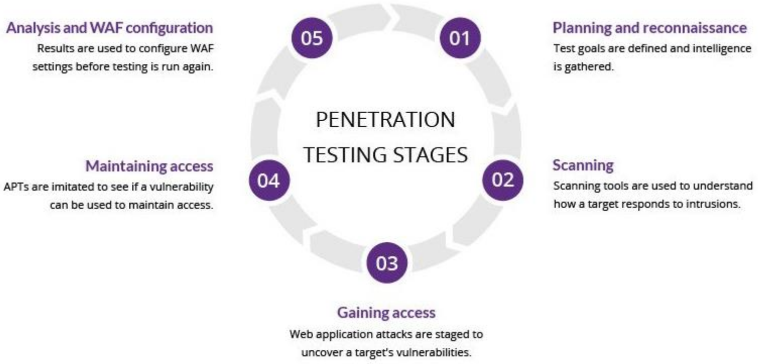
- After testing the network to understand its behavior, ethical hackers carry out a variety of attacks on the network, including web application attacks, SQL injections, and more. These attacks will help identify vulnerabilities in the targeted network. If ethical hackers find vulnerabilities, they try to exploit them, from trying to steal data to escalating privileges to intercepting traffic. The idea here is to determine how much damage they can do. Another interesting metric after successful access is how long testers can maintain their access in the system. If hackers can maintain access to a system for a long period, this gives them more opportunities to cause damage and collect valuable sensitive data.

4. **Analysis**

- After completing the testing activity, the penetration tester will analyze their results and create a report showing their findings. The report will provide actionable insights on vulnerabilities, actual exploitability, and opportunities for businesses to take the necessary remedial action before real hackers have a chance to exploit their systems.

5. **Executive Summary**

- The summary should provide a concise description of the business risks and the overall impact of the outcome on the business. By providing a non-technical, accessible analysis of the current security state, non-technical stakeholders can easily understand their overall security state and more easily provide needed support.



PENETRATION TESTING STAGES
01
Planning and reconnaissance
Test goals are defined and intelligence is gathered.
02
Scanning
Scanning tools are used to understand how a target responds to intrusions.
03
Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.
04
Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.
05
Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

6. **Risk Analysis**

- This section should walk through the risk findings, providing a detailed analysis of the discovered risks and their implications.

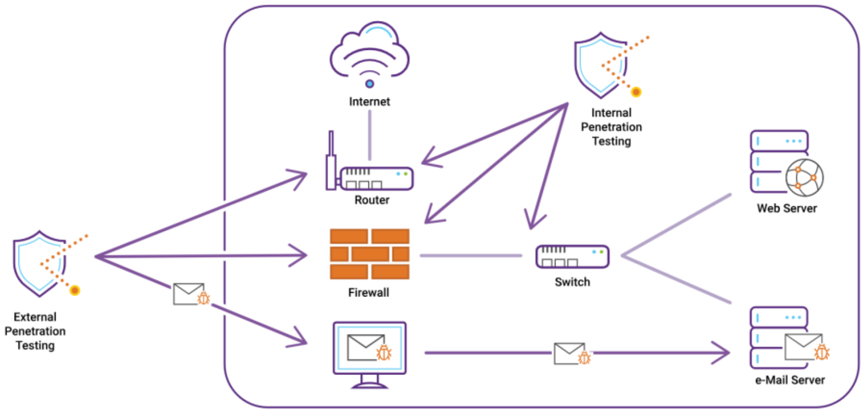
7. **Impact Analysis**

- This should include a detailed description of how likely it is that the discovered vulnerabilities will be exploited, and how damaging/widespread the impact will be if they are exploited at all.

8. **Remediation recommendations**

- This should offer the next steps the business can take to remediate discovered vulnerabilities and weaknesses.

Penetration Testing Picture:



- **Risk Assessments: Evaluate the potential impact and likelihood of various security risks to prioritize mitigation efforts.**

Network risk assessment looks at how these devices (such as computers, laptops, ipads, servers, routers, etc.) are managed. Some of these devices have modules that evaluate selected compliance, such as PCI and HIPAA compliance.

Tools used for Network Risk Assessment

- Performance Issues
- Security Risks and Issues
- Number of networks or servers used throughout multiple locations.

Case Study:

1. Unsupported Operating Systems

Issue: Computers were found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk.

Recommendation: Upgrade or replace these computers.

2. Anti-Virus Not Installed

Issue: Anti-virus software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.

Recommendation: To prevent both security and productivity issues, we strongly recommend assuring anti-spyware is deployed to all possible endpoints.

3. User Password Set to Never Expire

Issue: User accounts with passwords set never to expire, present a risk of use by unauthorized users. They are more easily compromised than passwords that are routinely changed.

Recommendation: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

4. Operating System in Extended Support

Issue: Computers were found using an operating system that is in extended support. Extended support is a warning period before an operating system is no longer supported by the manufacturer and will no longer receive support or patches.

Recommendation: Upgrade computers that have operating systems in extended support before the end of life.

➢ Security Audits: Review your network's security controls, policies, and procedures to ensure they align with best practices and compliance requirements.

Security audits are also known as internal audits or compliance audits. These audits are performed to assess the security of your company's information systems, but they are also performed to assess compliance with security regulations. The frequency of security audits may vary from company to company, but most organizations conduct them once a year.

Security audits can be divided into network security audits, web application security audits, blockchain security audits and other types. In this article, we'll discuss how cybersecurity audits can help protect you from today's cyberattacks and how important they are for achieving regulatory compliance.

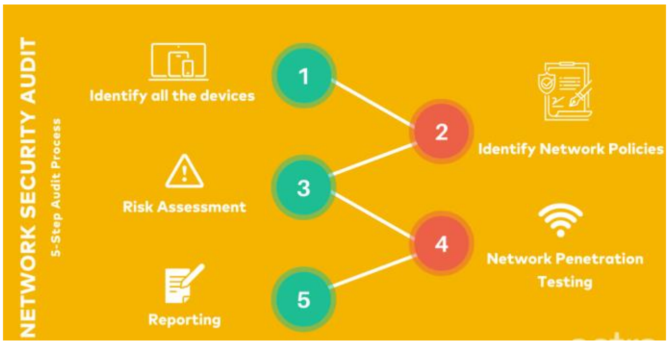
While we perform a network security audit

1. **Password Security**
   - Proper password policy
   - Use of password manager
   - Insecure storage of passwords
   - Common password usage

2. **Internal Network Security**
   - Proper access permissions
   - Disable guest accounts.
   - Log for unauthorized login attempts

3. **Firewall Security**
   - NAT Implementation
   - Inbound network rules
   - Firewall policies for security risks

4. **Mobile Devices Security**
   - Connected devices should be encrypted.
   - List of applications installed for verification of insecure apps.



- **Social Engineering Tests: Assess the susceptibility of your employees to phishing and other social engineering attacks.**

Social engineering penetration testing focuses on people and processes and the vulnerabilities associated with them. Ethical hackers often conduct These penetration tests for different social engineering attacks, such as phishing, USB drops, or impersonations that a person might face during their work. The goal of this test is to identify a weakness in a person, group of people, or process and identify the weakness through a clear path to remedy.

We perform a social engineering test:

On-site Tests

On-site tests are used to test the physical security of a building and to policies in place, like a clean workstation policy.

The typical methods of attack you would use for an on-site test are:

- Impersonation
- Dumpster Diving
- USB drops
- Tailgating

Off-site Tests

Off-site tests are used to test user's security awareness during their normal day. During this type of test, the pen tester will research the company and use information that is publicly available to test the company.

These tests are conducted remotely and commonly consist of the following attacks:

- Vishing
- Phishing
- Smishing

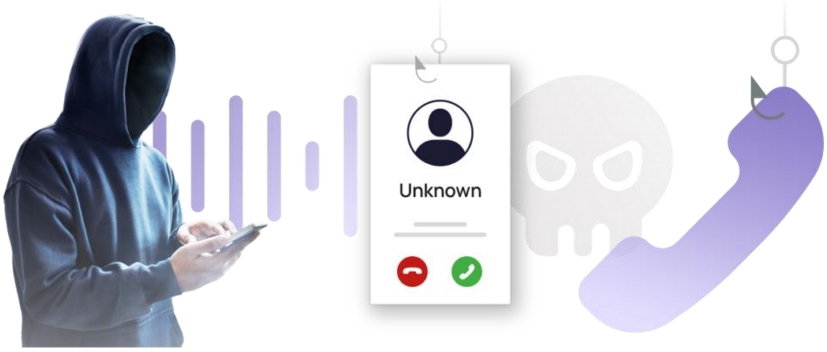
Case Study:

1. Phishing

Phishing is a method that occurs via email and attempts to trick the user into giving up sensitive information or opening a malicious file that can infect their machine.

2. Vishing

Vishing is like phishing but occurs via phone calls. These phone calls attempt to trick the user into giving up sensitive information.



3. Smishing

Smishing is like phishing but occurs via SMS text messages. These text messages have the same intent as phishing.

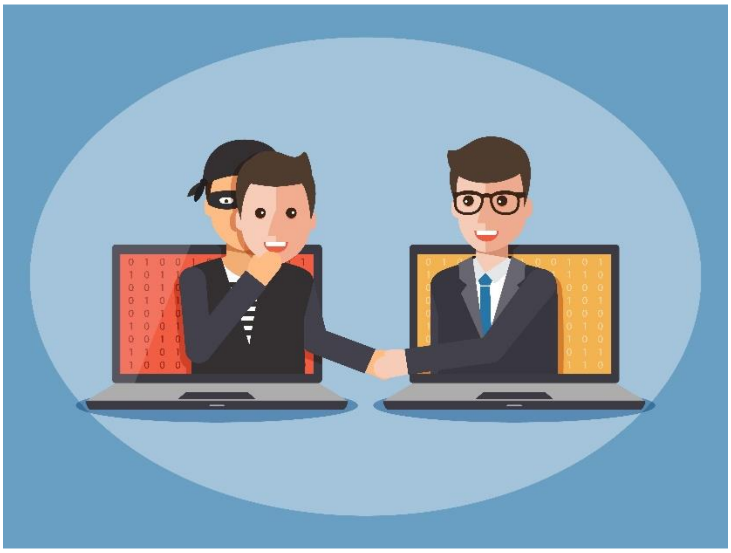
4. Impersonation

Impersonation is a method where the attacker attempts to fool a person into believing they are someone else.

For example, an attacker could impersonate an executive to convince employees to provide financial payments to fictitious vendors or to grant access to confidential information.

An impersonation attack could also target a user to gain access to their account. This could be accomplished by requesting a password reset without the administrator verifying their identity.

Another example of this attack would be pretending to be a delivery person. In some cases, delivery personnel have little restrictions and can gain access to secure areas without question.

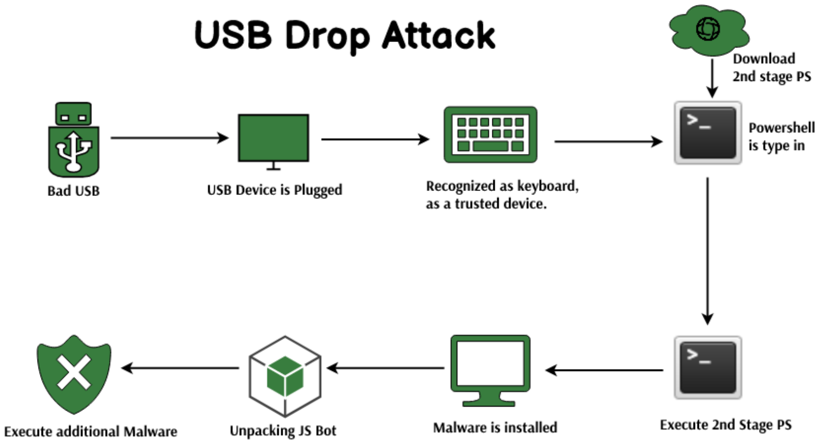


5. Dumpster Diving

Dumpster diving is a method where an attacker goes through not only trash but other items in plain sight, such as sticky notes and calendars, to gain useful information about a person or organization.

6. USB Drops

USB drops are a method that uses malicious USBs dropped in common areas throughout a workspace. The USBs typically contain software that, when plugged in, install malicious software that can provide a backdoor into a system or transfer files with common file extensions.



7. Tailgating

Tailgating is a method that is used to bypass physical security measures. You typically see this method used in locations that require a person to scan a key fob to gain entrance.

In this type of attack, the attacker will follow closely behind an employee and enter the room when they scan their key fob and open the door.

SAFE FROM TAILGATING
Keep a vigilant eye on visitors entering the building
Follow strict record-keeping procedures for visitors
Report the suspiciou activity

1.2 Firewall Implementation and Management

Firewalls are essential network protection tools that must be strong to the highest possible level. The implementation of network firewalls is a demanding task. Administrators need to maintain a perfect symmetry between end-user security and performance quality. Therefore, firewall configuration is also a key task for IT helpdesk outsourcing companies to determine the security reliability of their customers' networks.

A network firewall protects your data and devices from external threats and malware. Therefore, administrators should configure firewalls to protect your network under any circumstances. In addition, potential security threats should be considered when configuring a network firewall. It will keep your network secure from existing and future threats.

We perform implementation and management:

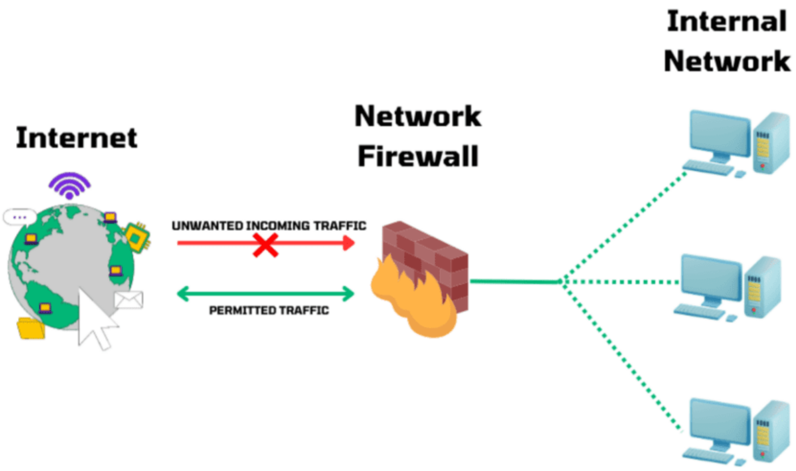
1. Set Automatic Traffic Control and Review User Access

An ideal security measure to block all traffic to your network automatically. You can allow explicit traffic only to certain known services. It will help you control access to your network and prevent any security violations from occurring.

Firewalls are the first step in network security against known and unknown threats. Therefore, you should not grant everyone permission to change the configuration. User access control must ensure that only approved supervisors have access to the firewall configuration.

In addition, each time an authorized executive makes a configuration change, it must be recorded in a log for review and observation. As a result, any unnecessary changes in the configuration can be noticed immediately, and a recovery can be performed in this case.

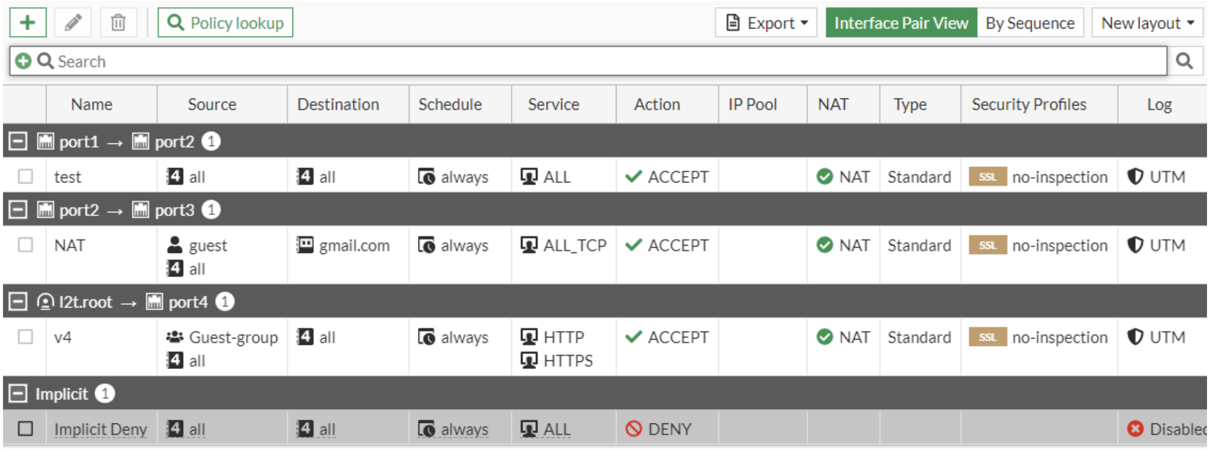
Again, you can create individual user accounts that allow different levels of access to your IT team. This way, you can provide only the access required for a job to a specific employee. In addition, you should monitor your firewall logs regularly. It will ensure that no unauthorized access to firewall Settings from internal or external networks remains unnoticed.



2. Amend the Rules of the network Firewall.

There must be well-defined rules in firewall security management. It will ensure proper network protection according to your needs and expectations. In addition, clearing out any unnecessary clutter in your firewall can have a positive impact on your network security.

Your firewall rule base may contain unnecessary components, duplicates, or too many rules that are not needed. This confusion makes the system complex and inefficient. It is therefore crucial to eliminate these useless rules and implement a set of clear guidelines that will lead to better outcomes.



	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles	Log
⊟	port1 → port2 1										
□	test	all	all	always	ALL	✓ ACCEPT		NAT	Standard	SSL no-inspection	UTM
⊟	port2 → port3 1										
□	NAT	guest all	gmail.com	always	ALL_TCP	✓ ACCEPT		NAT	Standard	SSL no-inspection	UTM
⊟	l2t.root → port4 1										
□	v4	Guest-group all	all	always	HTTP HTTPS	✓ ACCEPT		NAT	Standard	SSL no-inspection	UTM
⊟	Implicit 1										
□	Implicit Deny	all	all	always	ALL	DENY					Disabled

To keep your firewall rule base clean and up to date, consider the following:

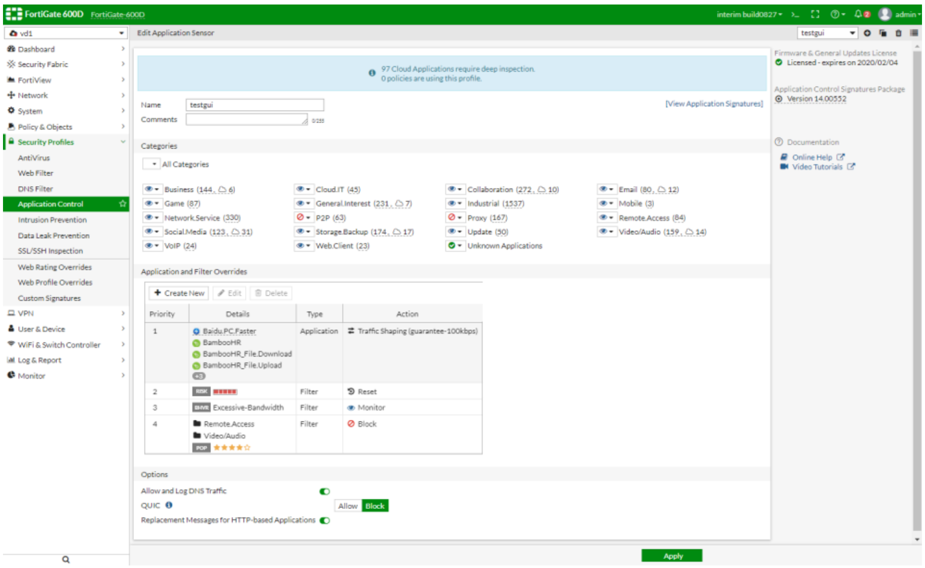
Unnecessary or duplicate rules cause the firewall to perform additional processing. It degrades the performance of the system, and it is better to eliminate these unnecessary rules.

Remove rules that are outdated and no longer applicable. These useless rules make your firewall management more complicated and can sometimes pose a threat to network security.

Unwanted rules can be confused with other critical rules, and the firewall manager can skip these useful rules. It may cause errors and failures in your firewall, so remove these suspicious rules promptly.

3. Revise Firewall Tools Regularly

Firewall service providers provide regular software updates. These updates have improved features to protect against new possible security threats. It is vital to keep your firewall software up to date not only to ensure the security of your network but also to detect any vulnerabilities in your system. Therefore, you must check from time to time to ensure that your firewall software is running the latest version.



Edit Application Sensor

97 Cloud Applications require deep inspection.
0 policies are using this profile.

Name: testgui
Comments: 0/255

[View Application Signatures]

Firmware & General Updates License
✓ Licensed - expires on 2020/02/04

Application Control Signatures Package
Version 14.00552

Documentation
Online Help
Video Tutorials

Categories

All Categories

👁 Business (144, ☁ 6)	👁 Cloud.IT (45)	👁 Collaboration (272, ☁ 10)	👁 Email (80, ☁ 12)
👁 Game (87)	👁 General.Interest (231, ☁ 7)	👁 Industrial (1537)	👁 Mobile (3)
👁 Network.Service (330)	⊘ P2P (63)	⊘ Proxy (167)	👁 Remote.Access (84)
👁 Social.Media (123, ☁ 31)	👁 Storage.Backup (174, ☁ 17)	👁 Update (50)	👁 Video/Audio (159, ☁ 14)
👁 VoIP (24)	👁 Web.Client (23)	✓ Unknown Applications	

Application and Filter Overrides

Priority	Details	Type	Action
1	Baidu.PC.Faster BambooHR BambooHR_File.Download BambooHR_File.Upload +3	Application	Traffic Shaping (guarantee-100kbps)
2	RISK ■■■■■	Filter	Reset
3	BHVR Excessive-Bandwidth	Filter	Monitor
4	Remote.Access Video/Audio POP ★★★★☆	Filter	⊘ Block

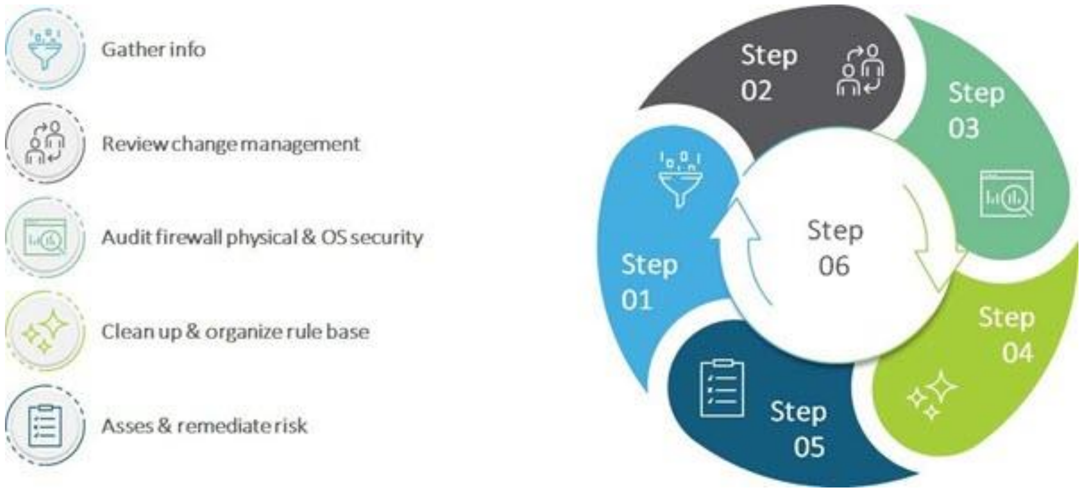
Options

Allow and Log DNS Traffic ●
QUIC: Allow [✓ Block]
Replacement Messages for HTTP-based Applications ●

4. Conduct Regular Audits of Firewall

A security check of your network is essential to confirm that your firewall restrictions follow corporate and external security rules. Any unauthorized change in the firewall configuration is a violation of the policy and may result in non-compliance. Administrators and IT security teams need to perform regular security checks to ensure that there are no unauthorized modifications in the system.

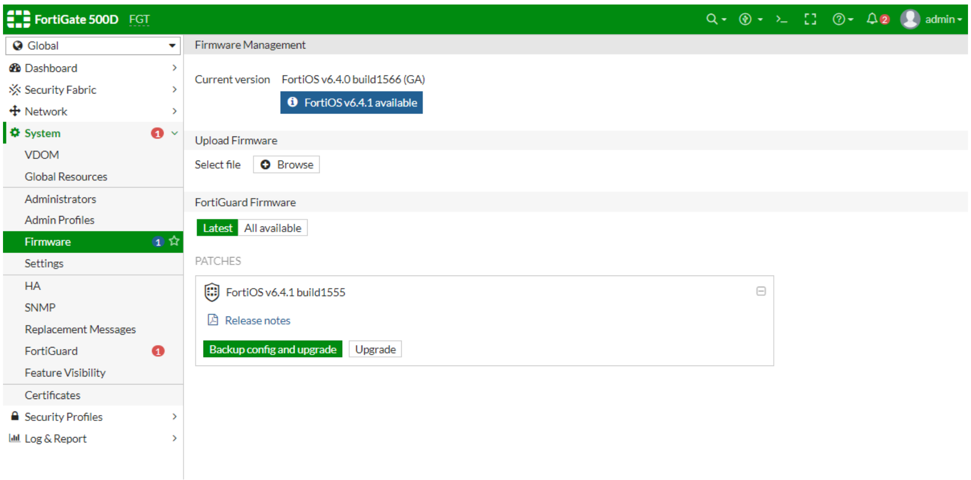
These systematic measures will help you keep abreast of important changes made to your firewall. It will also be aware of any risks that may arise because of these modifications. Security checks are of the utmost importance when installing, migrating a new firewall, or making major configuration changes.



5. Perform Updating of Firewall.

Enhanced technologies have made IT processes fast and effortless. At the same time, your firewall administrators may not regularly review and update the firewall software. It may result in a security breach leaving your network at risk.

You can automate the updating process of your firewall to avoid such situations. An automated process can check if there is any update available in the system and execute the same as per the schedule. This process brings efficiency to your security management process.



Current version FortiOS v6.4.0 build1566 (GA)

FortiOS v6.4.1 available

Select file

FortiOS v6.4.1 build1555

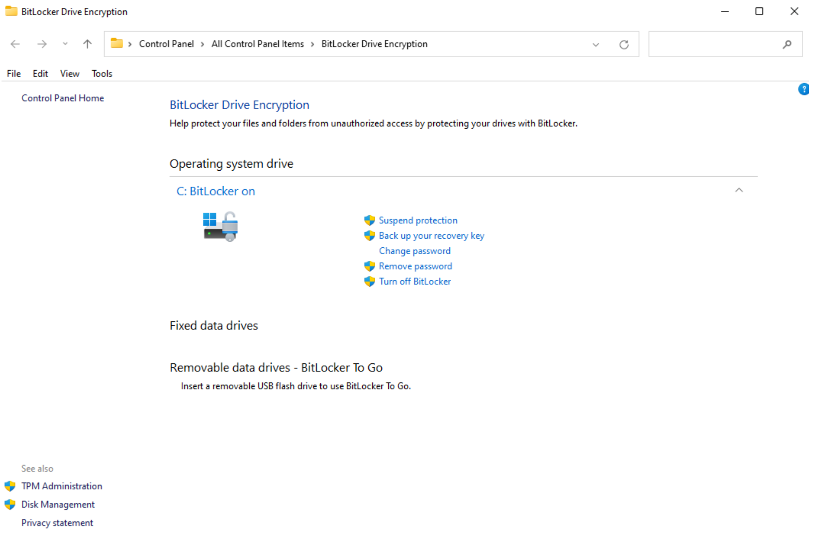
1.3 Data Encryption Services

Data encryption is a crucial aspect of modern data security. There are several ways to implement data encryption services, depending on your specific needs and the nature of the data you want to protect.

We perform data encryption services:

1. Full Disk Encryption

We will encrypt an entire disk or storage device, ensuring that all data stored on it is protected. Operating systems like Windows and macOS offer built-in full disk encryption features.



BitLocker Drive Encryption

Control Panel › All Control Panel Items › BitLocker Drive Encryption

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker on

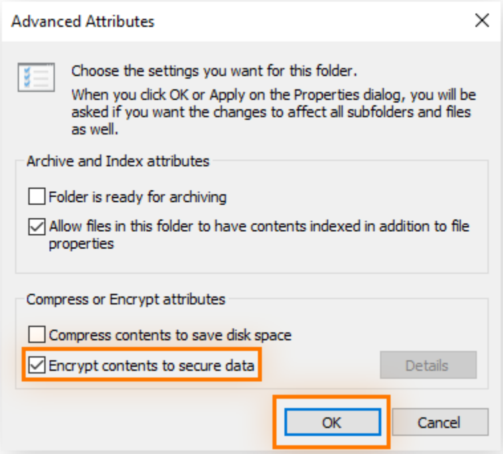
Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

2. File-level Encryption

We can encrypt individual files or folders, giving us more granular control over protected data. Tools such as BitLocker for Windows or File Vault for macOS are available for file-level encryption.



Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☐ Folder is ready for archiving

☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

☐ Compress contents to save disk space

☑ Encrypt contents to secure data

3. Cloud Storage Encryption

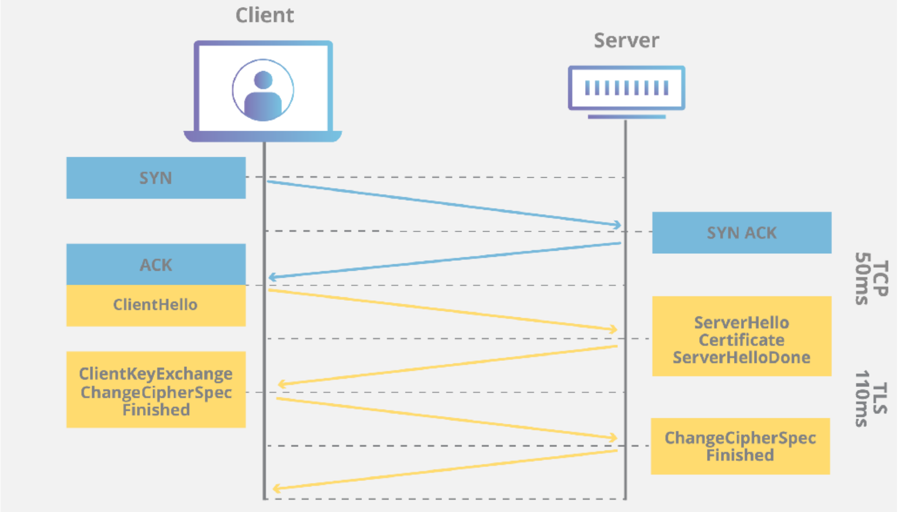
We may use the encryption capabilities of the cloud storage provider or implement client-side encryption to help protect your data from unauthorized access.

4. End-to-End Encryption

We ensure that data is encrypted from the point of origin to the point of consumption, preventing intermediaries from accessing unencrypted data. It is commonly used in messaging applications and communication platforms.

5. Transport Layer Security (TLS)

We will implement the TLS protocol, which can ensure that data is encrypted during transmission, preventing eavesdropping and tampering.



1.4 Endpoint Security Solutions

Endpoint security is the practice of protecting the data and workflows associated with the individual devices connected to the network. The Endpoint Protection Platform (EPP) works by checking files as they enter the network. Modern EPPs leverage the power of the cloud to hold a growing database of threat information, freeing endpoints from having to store all this information locally and keeping those databases up to date with the required maintenance. Accessing this data in the cloud also allows for faster speed and scalability.

EPP provides system administrators with a centralized console that is installed on a network gateway or server, allowing network security professionals to remotely control the security of each device. The client software is then assigned to each endpoint - it can be delivered as SaaS and managed remotely or installed directly on the device. Once the endpoint is set up, the client software can push updates to the endpoint as necessary, verify login attempts from each device, and manage company policies from one location. EPP protects endpoints through application control (which prevents the use of insecure or unauthorized applications) and encryption (which helps prevent data loss).

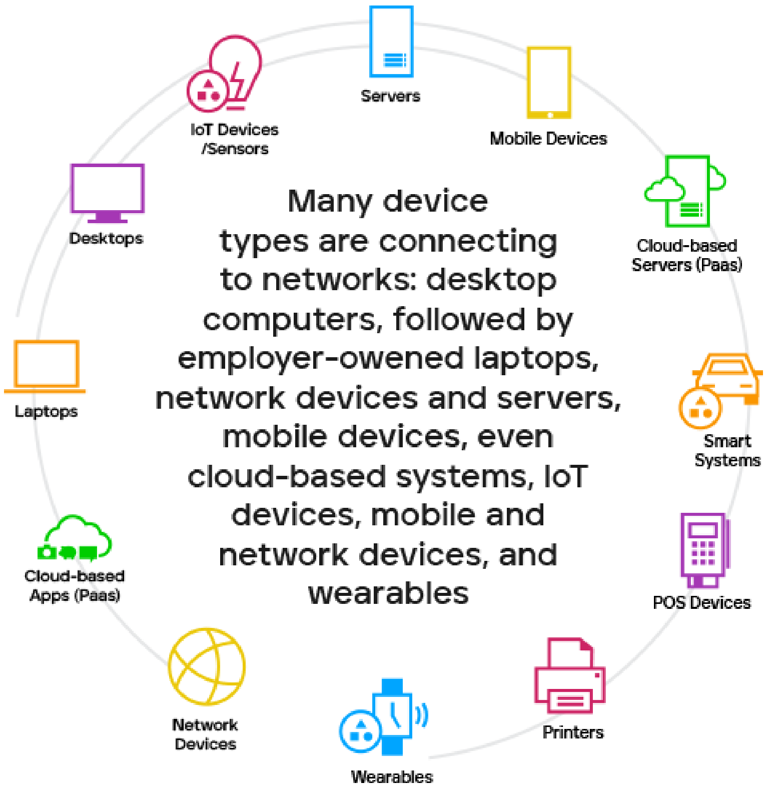
Once EPP is set up, it can quickly detect malware and other threats. Some solutions also include endpoint detection and response (EDR) components. EDR capabilities allow detection of more advanced threats, such as polymorphic attacks, fileless malware, and zero-day attacks. By employing continuous monitoring, EDR solutions can provide better visibility and multiple response options.

EPP solutions can be used in on-premises or cloud-based models. While cloud-based products are more scalable and can be more easily integrated with your current architecture, some regulatory/compliance rules may require on-premises security.

If a device is connected to a network, it is considered an endpoint. With the growing popularity of BYOD (Bring Your Device) and IoT (Internet of Things), the number of personal devices connected to an organization's network can quickly reach tens (or even hundreds) of thousands.

The range of endpoints can range from more common devices such as:

- Tablets
- Mobile devices
- Printers
- Servers



Many device types are connecting to networks: desktop computers, followed by employer-owened laptops, network devices and servers, mobile devices, even cloud-based systems, IoT devices, mobile and network devices, and wearables

1. Endpoint security identifies and classifies your assets

The EDR tool tracks and records all activities and events that occur on the endpoint. It provides endpoint security solution teams with an overview of network performance, revealing events that are undetectable to the naked eye.

2. Endpoint to implement user activity monitoring

User activity Monitoring (UAM) is a key component of endpoint security. Its endpoint security solutions enable you to know which users are accessing which data, when and from where. Information from UAM is used to identify suspicious activity and prevent data breaches. Its endpoint security solution can also detect insider threats and breaches.

3. Use device management tools and MDM endpoint security solutions

Mobile Device Management (MDM) is a type of security software that helps businesses secure and manage mobile devices such as laptops, smartphones, and tablets. An MDM Endpoint Security solution typically includes remote device management, device registration, policy management, and security control. By implementing an MDM solution, organizations can control employee-owned devices and ensure that only authorized devices can access enterprise data.

Device management tools give you the ability to manage and monitor endpoints remotely. With these tools, you can:

- Deploy updates and patches,
- Track device location,
- Remotely wipe devices if they're lost or stolen and lock down devices if necessary.

4. Install a Reputable Endpoint Antivirus Program

Endpoint Security Solutions Antivirus software protects your computer from malware such as viruses, worms, and Trojans. Businesses must install reputable antivirus programs on all endpoint devices to prevent malware from infecting corporate systems.

5. Use Strong Authentication Techniques for Endpoint Security

One of the best ways to improve endpoint security is to rely on strong authentication techniques. It has become a necessity in today's business world. To keep corporate data secure, companies should require employees to use strong passwords and two-factor authentication when remotely accessing corporate resources.