Identity-Based Security: An Imperative for Cyber Security

Abstract:
Identity-based firewall provides a means through which administrators can uniquely identify users, control Internet activity of these users in the network, and enable policy-setting and reporting by username. It utilizes the eight layer or the “human layer” in the network protocol model. This therefore provides identification of attackers or their victims with username, insight for administrators into the source of attacks, great control over who is carrying out a particular activity in the network, creation of identity-based policies and reporting measures to track identity-based usage, problems and several intrusions. The awareness of user identity and group information is very important to most theoretical and all practical models of digital identity secure access to resources and data, which may reside in various data centres. The application of users’ ID allows the next-generation firewall to consistently enforce policies based on users, their location, time of access, type of device notwithstanding. This provides identity-based security, enterprise-wide visibility and deep monitoring of user activity based on specific users and groups rather than Internet Protocol addresses alone. Layer eight firewall provides a strong foundation on which an organization can adopt security and curtail the success of cyber security threats.

Keywords: Firewall, cyber security, network, identification, intrusions, policy

1. Introduction
It needs a change in the area of mobile evolution from the way business generally applies it and manages it for securing networks. As administrators are accountable for each possible area of users, rules of firewalls becoming very stringent as it needs IP addresses. More security is needed irrespective of location of users. Security policies aim to provide more flexible, accurate control in case of accessing the network. Identity-based firewall security, as it is based on user as well as group at the point of access, provides more stretchy access control. According to Powel (2012), more security, flexibility of usage, less strict maintenance policies are some of the advantage of this system. IBM’s 2014 “Cyber security Intelligence Index” revealed that human error or a breached identity is about 95% among all kinds of security (Veronica, 2015). This issue many times become problematic to handle as it involves many stakeholders like business partners, suppliers and contractors as well as third-party service providers with many secretarial constitutional rights. As per International Business Machine’s Cyber Security Intelligence Index, 2014, lack of control may lead to security breaches. The traditional firewall systems are basically made to filter traffic based on IP addresses, source and destination ports and protocol types; whereas, new networks have been designed in such a way such that the likelihood for users’ mobility is a necessity requirement. This gives more intricacy as management becomes exasperating with the involvement of firewall administrators. As a solution, an identity-based firewall system uses the user’s identity to filter the traffic. According to Nenad and Marjan (2011), intersection of people, devices and application has been made possible with this security based on identity.

2. Security Provisions of Identity Based Firewall
A boulevard to control access can be created by the Identity-based security while permitting access to a digital product or service. This can allow organizations to provide permissions to many institutions for contacting users to access a variety of digital services using the same credentials, with exact match between what users are permitted to and what they in reality obtain (Identity & Access Management, 2016) with many restrictions like company, device, location and application type attributes (Linthicum, 2014). The identity-based access control -IBAC or identity-based licensing is a part
of the identity-based security approach (What is Identity, 2016; Adobe Systems, 2008). As per, National Institute on Standards and Technology (NIST), Identity-based Security policies are based on the identities and/or attributes of the system resource which can be accessed by user, group of users, process, or device (Gary, 2001). Many advantages have been highlighted by many authors like Enrico (2003), Powell (2012) etc. encouraging access to wide range of smartphones, tablets, and PCs is one of the attractive advantages. Cyberoam is a typical example of Identity-based security network security approach. It manages user activity for a certain network. It has human identity as a component of the firewall rule matching criteria (Cyberoam, 2019). While checking for authentication, authorization and auditing, it treats user’s identity as the eighth layer (also known as the human layer) as a protocol in aspecific network layer. It gives more accurate control over who can access the network and what they can be really accessed. It provides an opportunity to institutions to form security policies that consider users and groups instead of IP addresses. Encryption, authentication, and access control prevents from address spoofing attacks. Thus, it is more secure than inheritance platforms of mobile devices.

According to Powel (2012), network resources can be accessed from specified from terminals or workstations as it has capability to enforce policies. This creates huge growth in the personal or mobile devices. Control and audit access web resources on mobile devices have been offered by the Next-Generation Firewall (layer 8). It doesn’t require any type of installed software on mobile. Uniform Resource Locator (URL) and key in their username and password are the only things needed to access the applications and data which are privileged.

Identity-based architecture helps to provide the right applications to the right users on any computing machine. It also links with user identity repositories they want to use for enforcing rules. Thus, it ensures centralized management and auditing. Next-Generation Firewall (layer 8) protects institutions from Denial of Service (DoS), Distributed Denial of Service (DDoS) and IP Spoofing attacks by applying deep packet inspection for network, application and user identity-based security. Establishing the core principle of identity as security in one’s organization will provide a means of survival against cyber threats. Identity-based security could be through identity and access management (IAM) or with Privileged Account Management (PAM) approaches which provides a first layer of control. A circle of trust cannot be depended on if one does not have the identity aspect strongly guarded. Hence, defending the identity must be the first layer in one’s security system because if one can protect identity, one has a better position at protecting the endpoints and network at large. Therefore, using identity and access management, Layer 8 firewall provides powerful enhancements that thereby provide a simpler means through which organizations of all sizes can control access to their resources based on user identity, ensuring that only the right users have access to the right resources always.

3. Features of Identity-based Firewall Security

According to Powell (2012), Identity-based firewall security furnishes advanced features that lessen costs and operational obscurity as well asrising securityin general. These include:

- Stipulation of an affluent policy language: This enables effectual manage of users and groups while tumbling the total number of access regulations. Policies are seen as business rules, hence are easy to employ and administer. As a result of this, more control is attained though fewer policies are requisite.
- Enforcement of Identity-based policy: This aligns policies to user and group instead of IP address, enabling policy organization across local and remote users and supports identity-enabled control of threats.
- It seamlessly works across multiple devices.
- It is such that it can be used to enforce access control policy across several access points such as smartphones, tablets, and personal computers.
- Simplified configuration of policy: IDs can be chosen from an existing directory of users and groups;thus,policy creation and enforcement are easier.
- Context-aware security feature which provides organizations with the ability to determine who is trying to access a given content; the location and time of the attempted access; and the type of application and device that is being used.
- Provision of simplified business policies that blends with Information Technology enforcement needs and the business rules of an organization.

Table 1 below shows the characteristics of a Typical Layer 8 Firewall.

---

Table 1: Characteristics of a Typical Layer 8 Firewall

| Feature                                      | Description                                                                 |
|----------------------------------------------|-----------------------------------------------------------------------------|
| **Identity Management**                      | Provides user authentication, authorization, and auditing.                  |
| **Access Control**                           | Enables enforcement of access policies.                                     |
| **Mobile Device Access**                     | Supports access from mobile devices.                                        |
| **Identity-based Enforcement**               | Blends with Information Technology enforcement needs.                       |
| **Centralized Management**                   | Enables centralized management and auditing.                                |
| **Protection from Threats**                  | Offers protection from Denial of Service (DoS), Distributed Denial of Service (DDoS), and IP Spoofing attacks. |
| **Deep Packet Inspection**                   | Applies deep packet inspection for network, application and user identity-based security. |
| **Flexibility across Devices**               | Works seamlessly across multiple devices.                                   |

---
| Feature Description | Benefit |
|---------------------|---------|
| **Human Layer 8 Identity-based Security Features** | **Benefit** |
| • Firewall with Identity-based policy creation | • Secures dynamic IP environments like Wi-Fi and instances where users share the endpoints |
| • Access Control Criteria (ACC) – User-Identity, Source & Destination Zone, MAC and IP address, Service | • User identity-based decision making prevents errors associated with IP address-based policies |
| | • Simplifies audit requirements with instant user identification |
| **FUSION Technology** | **Benefit** |
| • Policy creation for multiple security features through single interface in firewalls | • Blends Security, Connectivity, Productivity |
| • Firewalls well-integrated with VPN, IPS, Anti-Virus & Anti-Spyware, Anti-Spam, Web Filtering, Bandwidth Management, Multiple Link Management | • Provides integrated perimeter security |
| **Thin Client Support** | **Benefit** |
| • Thin client authentication with session IDs | • Supports SaaS deployments and Cloud environment |
| • Supports Citrix –XenApp server, Microsoft Windows Server (Microsoft TSE) | |
| • Identity-based policies in thin client environment | |
| **Enterprise-Grade Security** | **Benefit** |
| • Firewall with High Availability with stateful failover | • Faster up-times, reduced latency, simplified configuration, supports rapid network growth |
| • Available as Next-Generation Firewalls and UTM’s | • Supports creation of work profile-based groups across distributed locations |
| • Multiple Security Zones | • Enables secure hosting of servers inside LAN and DMZ, efficient use of limited public address pool to host services |
| • Firewall appliance offering Dynamic Routing | • Supports applications that work on real-time updates like stock updates for financial institutions |
| • VLAN support | • High throughput |
| • Virtual host capability | |
| • Multi-casting | |
| • Multi-core technology allows high-speed parallel processing | |
| • ICSA-certified firewalls | |
| • Checkmark Level 5 Certified | |
| **Centralized Management** | **Benefit** |
| • Centralized Security with CCC | • Simplified security management |
| **Logging & Reporting** | **Benefit** |
| • Layer 8 Identity-based Reporting | • Meets compliance requirements for CIPA, HIPAA, PCI DSS |
| • Firewall logs | |
| • Centralized logging and reporting with Cyberoam iView and CCC | |

Table 1: Characteristics of a Typical Layer 8 Firewall  
Source: Cyberoam (2019)

3. Key System Capabilities in Identity-based Security  
To control the data of an entity for use by applications, these system capabilities are necessary.  
- Authentication: as per *Mahfouz, Mahmoud, and Eldin* (2017), this is a confirmation that an unit is who or what it claims to be using a password, biometrics such as a fingerprint, or any unique actions such as a gesture pattern on a touchscreen.
• Authorization: organization of authorization information that defines what operations a unit can carry out in the context of a specific application. An example is when one user is endorsed to enter a sales order, while an additional user is endorsed to acclaim the credit demand predestined for that order. (Jøsang, 2017).

• Roles: These are collections of operations. Roles often connected to a scrupulous job or job function contracted to users. An example is where a user superintendent role might be sanctioned to rearrange a user’s password, whereas a system supervisor role will have the ability to allocate a user to a meticulous server (Abreu, Santin, Viegas and Stihler, 2017).

• Delegation: This allows local administrators to modify systems without a global administrator. Also, a user may allow another to perform actions for them. An instance is when a user gives the right to information related to office (Barka and Sandhu, 2000).

4. Controlling Insider Threats with Identity-Based Security

Veronica (2015) states that identity and access management solutions can help address the problem of both negligent and malicious activity. All user groups with internal access to business systems should be certified and monitored, and each user's access to corporate data should be mapped to align with their job requirements and responsibilities. It should be ensured that access privileges align with established security policies and are backed up by auditing tools to monitor and report on user behavior. They can also help control policy violations and identify abuse that could signal an insider threat. The privileged identity, with its access to IT resources and ability to delete traces of its activities, remains a big concern. If a privileged identity is not properly managed, it can cause security vulnerabilities and compliance issues and increase the risk of data theft. Privileged identity management solutions that control and monitor access of users while providing individual user accountability should be considered.

Veronica (2015) equally notes that when integrated with identity and access management, a security intelligence solution can produce user analytics and highlight anomalies, enabling organizations to do the following:

• Establishment of a baseline for user behavior and quick detection of anomalies;

• Creation of alerts when anomalous behavior is noticed;

• Correlation of identities with known threats or suspicious IP addresses;

• Protection against insider fraudulent activities by highlighting employee accounts that are compromised.

When the right security solutions are applied, organizations will be able to strengthen their identity management in such a way as to minimize insider threats and improve compliance.

Harinder and Gurpreet (2013) note the following issues concerning common threats in multi-user environment and shared access of data by different users:

• The identity is based upon machine (Media Access Control) or IP not by person: These computers on a network are identified by their IP or MAC address only and not by the identity of the person that is using it. Users can use the computers to use websites and contents that are restricted by the organization by using the IP address as coverage, thus making it impossible to be able to track the person that has done that.

• “Coconut” security: The security is hard from outside and soft from inside, thus computer networks are made secure from outside threats while ignoring the insider threats. The user is the biggest insider threat that can create problems and breach security since they lack security awareness. Thus, the organization may not be able to record the person that is accessing a given portion of data until a security breach has taken place.

• The security model is reactive and not proactive.

Present day multi-user environments have enormous security issues. Since the security settings are for the system not for the user, it becomes impossible to track down the activities of a particular user. The user’s activity is changing and could become inappropriate either intentionally or unintentionally hence could easily become victim of cybercrime. A user's neglect to warnings can cause network security breaches (Harinder and Gurpreet, 2013). Common issues regarding the network or internet in multi-user environment according to Harinder and Gurpreet (2013) are:

• Heavy uploading and downloading which slows down the network.

• Online gaming which causes slowdown of network.

• The use of instant messaging.

• Consumption of bandwidth leading to limited bandwidth.

• Having access to information.

Sequel to these concerns, Harinder and Gurpreet (2013) note the following benefits of Identity Based Security

• The user’s network access is based on user authentication with a pre-defined user profile, not on machine (MAC) or IP and this can help to check who is doing a particular thing and when it is being done.

• Provision of proactive defense such that threats could be analyzed by auditing the data obtained from previous sessions.

• Ability to know the application consuming bandwidth or the web site that is visited often.

• Helping administrators to view what is happening over the network such as the applications that are accessing the network in such a way that if a user or an application is trying to perform an unauthorized activity, it could be prevented.

• Recording of the downloading and uploading activities of a user in every session,

• Monitoring the number of users accessing the network at a specific time.

• Proper management of bandwidth.
• Internet quota management ensuring a limitation over the amount of data which a user can download or upload through the internet.
• Filtering of content is based on keywords.
• Websites that distribute proxies and malware are blocked.

5. Identity Management in Identity-Based Security

In Identity management, information about users on computers is controlled. Such information includes information that authenticates the identity of a user, and information that describes information and actions they are authorized to access and/or perform. It also includes the management of descriptive information about the user and how and by whom that information can be accessed and modified. Managed entities typically include users, hardware and network resources and even applications. It is a set of operations on a given identity model, or more generally as a set of capabilities with reference to it. It can also express how model contents are to be provisioned and reconciled among multiple identity models.

Digital identity is an entity’s online presence, encompassing personal identifying information (PII) and ancillary information (Fred, 2007; National Institute of Standards and Technology, 2009). It can be interpreted as the codification of identity names and attributes of a physical instance in a way that facilitates processing (The Center for Democracy & Technology, 2007).

Digital identity management as seen from the real-world context of engineering online systems can involve four basic functions as seen below:

• Pure identity function which involves the creation, management and deletion of identities;
• The user access function;
• The service purpose which is a system that delivers personalized role-based, online, on-demand, multimedia and presence-based services to users and their devices.
• According to Gaedke, Johannes and Nussbaumer (2005), Identity Federation, a scheme that depends on federated identity in order to legalize a user without significant his or her password.

As per Wehmeier (2012), such identities carry a particular relationship similar with real world. Generally, small set of axioms create a model of identity. "Pure identity" means a model which is not restricted by any constraints. Generally, a real or virtual entity can have multiple identities and each identity can include multiple attributes, some of which are distinctive within a given name space. A finite set of properties create identity object. The properties record information about the object, either for purposes external to the model or to operate the model, for example in classification and retrieval. Any sort of external semantics is not strict associated with a “pure identity” model.

The most widespread exodus from “pure identity” in practice occurs with properties planned to guarantee some aspect of identity, for example a digital signature or software token which the model may use from within to verify some aspect of the identity in satisfaction of an external purpose (Gartner IT Glossary, 2016). This situation may conflict with purposes of information security such as managing access or entitlement. These can be simply maintained and retrieved and not required any special treatment by the model. Identity management provides user access which facilitates users to presume a precise digital identity across applications; hence access controls can be assigned and evaluated against this identity. A single identity for a given user across multiple systems facilitates tasks for administrators and users. Monitoring and verification as well as it allows the institutions to curtail unnecessary privileges approved to one user. According to IBM Cloud Docs (2018), User access can be checked from instigation to extinction of user access. The main objective of an institution while implementing an identity management process or system is to provide suitable managing rights. Access managing is usually the inspiration for identity management and the two sets of processes are accordingly strongly connected (Search Security, 2018). For both internal users and customers, institutions add services. Identity management requires many services. Gradually more identity management has been alienated from application functions so that a single identity can provide many or even all of an organization’s activities.

Identity management as an internal use is growing to control access to all digital assets, including devices, network equipment, servers, portals, content, applications and/or products. Services need privilege to gain access into address books, preferences, entitlements and contact information. Donaldson and Lohr (1994), mentioned that mostly this information is needed to ensure privacy and confidentiality, controlling access. Identity-based security is allowing users to log in based on the authentication against one of the systems participating in it by using identity federation which consists one or more systems that unite user access. Among many systems there exists “Circle of Trust” which acts as the Identity Provider (IdP) while the other system(s) acts as Service Provider (SP). This implies that user needs admittance over some service prescribed by SP foe which, first he or she first authenticates against the IdP. Next, the IdP sends a secure “assertion” to the Service Provider for affluent confirmation. The Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization of data between parties, in particular, between an identity provider and a service provider. The assertions can be used by whoever is verifying to make a statement about the identity of a claimant and may be optionally signed digitally (Burr, Donaldson, Folk, 2006).

6. Conclusion

The relevance of an Identity-based security in a cyber-security system cannot be over-emphasized. The approach is very pertinent in controlling access to a digital product or service based on the authenticated identity of an individual. As a result of this, organizations can grant access to specific users to access a variety of digital services using their credentials, ensuring the accurate match between what users are entitled to and what they actually receive. Hence,
appropriate access rights can be granted to those entities through their identities while also ensuring several access constraints such as device, location and application type attributes.

7. References
   i. Abreu, V.; Santin, A. O.; Viegas, E. K.; Stihler, M. (2017). A multi-domain role activation model(PDF). ICC 2017 2017 IEEE International Conference on Communications. IEEE Press. pp. 1–6. Doi: 10.1109/ICC.2017.7997247. ISBN 978-1-4673-8999-0.
   ii. Adobe Systems. 2008-05-01"Adobe Flash Media Rights Management Server 1.0 Overview for Microsoft Windows, Linux, and UNIX" (PDF). Workflows - Identity-based licensing. Archived (PDF) from the original on 2017-08-29. Retrieved 2017-11-14.
   iii. Barka, E.; Sandhu, R.: A role-based delegation model and some extensions. In: Proceedings of 16th Annual Computer Security Application Conference, New Orleans, U.S.A. (December 2000)
   iv. Burr, Donaldson and Polk (2006) (2006). "Information Security"(PDF). CiteSearX 10.1.1.153.2795. Doi: 10.6028/NIST.SP.800-63v1.0.2. Retrieved 10 October 2015.
   v. Cyberoam. "Security built around the user's identity". Retrieved 10 January 2019.
   vi. Donaldson, Molla S.; Lohr, Kathleen N. (1994)Confidentiality and Privacy of Personal Data. Networks, Institute of Medicine (US) Committee on Regional Health Data, National Academies Press (US).
   vii. Enrico, S. (2003). ".NET Identity and Principal Objects": informIT. Pearson Education. Archived from the original on 2017-11-14. Retrieved 2017-11-14.
   viii. Firewall security extended to Layer 8 https://www.cyberoam.com/firewall.html
   ix. Fred, C. (2007) Functional requirements for privacy enhancing systems, OECD Workshop on Digital Identity Management, Trondheim, Norway, 9 May 2007 (PPT presentation)
   x. Fred, C. (2007) Functional requirements for privacy enhancing systems, OECD Workshop on Digital Identity Management, Trondheim, Norway, 9 May 2007 (PPT presentation)
   xi. Gaedke, Martin; Johannes, Meinecke; Nussbaumer, Martin (2005). A Modelling Approach to Federated Identity and Access Management (PDF). Special Interest Tracks and Posters of the 14th International Conference on World Wide Web. Association for Computing Machinery. pp. 1156–1157. Doi: 10.1145/1062745.1062916. ISBN 978-1595930514
   xii. Gartner IT Glossary (2016) Identity and Access Management (IAM)". Gartner. Retrieved 2 September2016.
   xiii. Gary, S.SP 800-33 - Underlying Technical Models for Information Technology Security, p. 21, December 2001, NIST Computer Security Publications - NIST Special Publications (SPs), doi:10.6028/NIST.SP.800-33. Retrieved 4 April 2017.
   xiv. Harinder, P. S. and Gurpreet, K. (2013). Network Security: Identity Based Access Layer (8 Technology). International Journal of Computer Science and Communication Engineering IJCSCE Special issue on “Recent Advances in Engineering & Technology” NCRAC 2013 ISSN 2319-7080. www.ijcsc.e.org
   xv. IBM Cloud Docs (2018). console.bluemix.net. Retrieved 3 December 2018.
   xvi. Identity and Access Management: Pillars for effective Personalisation(PDF). 10duke.com. 2016-02-08. Archived (PDF) from the original on 2017-07-05. Retrieved 2017-11-14.
   xvii. International Business machine (IBM)’s Cyber Security Intelligence Index (2014). https://www.ibm.com/services/US/en/it-services/security-services/2014-cyber-security-intelligence-index-infographic.
   xviii. Josang, Andun (2017), A Consistent Definition of Authorization, Proceedings of the 13th International Workshop on Security and Trust Management (STM 2017)
   xix. Linthicum, D. (2014). "Analyst Report: Identity-based security and the cloud". Gigaom. Archived from the original on 2016-06-24. Retrieved 2017-11-14.
   xx. Mahmoud, A. M.; Mahmoud, T. M.; Eldin, A.S. (2017). "A survey on behavioral biometric authentication on smartphones". Journal of Information Security and Applications. 37: 28–37. doi:10.1016/j.jisa.2017.10.002.
   xxi. National Institute of Standards and Technology (2009) Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Recommendations of the National Institute of Standards and Technology, January 2009.
   xxii. Nenad Stojanovski, Marjan Gusev (2011)Architecture of an Identity Based Firewall System International Journal of Network Security & Its Applications July 2011, Volume 3, Number 4 ISSN: 0975- 2307
   xxiii. National Institute of Standards and Technology-NIST (2017) "Glossary: Identity-Based Access Control”. Computer Security Resource Center. Retrieved 2017-11-14.
   xxiv. Powell J. E. (2007) Next Generation Firewall https://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/at
   xxv. Powell, James E. (2012). "Q&A: Addressing BYOD with Identity-Based Security". Enterprise Systems Journal. Archived from the original on 2017-11-14. Retrieved 2017-11-14.
   xxvi. Security(2018)"What is identity management (ID management) ? - Definition from WhatIs.com”. Search Security. Retrieved 3 December 2018.
   xxvii. The Center for Democracy & Technology (2007). PII (Personally Identifiable Information) Archived 28 April 2009 at the Wayback Machine. The Center for Democracy & Technology, September 14, 2007
xxviii. Veronica, S. (2015) To Err Is Human: Why Your Users’ Identity Is Your Security’s Securityintelligence.com

xxix. Wehmeier, Kai F. "How to live without identity—and why," Australasian Journal of Philosophy 90:4, 2012, pp. 761–777.

xxx. "What is identity-based licensing?". 10duke.com. 2016-02-02. Archived from the original on 2017-11-14. Retrieved 2017-11-14.