Cisco Identity-Based Firewall Security

What Is the Value of Cisco Identity-Based Firewall Security?

Work has evolved from a place you go to something you do. The workforce is becoming increasingly mobile, often with around-the-clock connectivity provided through a broad range of devices that can be located anywhere in the world. This evolution requires a fundamental shift in the way businesses think about and administer network security. Legacy firewall rules that require the use of IP addresses have become more cumbersome as administrators must account for every possible location for each user. More granular controls are required to provide secure access to the network, regardless of a user's physical location, without adding undue complexity.

Security policies that align to users and groups rather than to IP addresses give organizations easier, more precise control over who can access the network–and what they can access. Cisco® identity-based firewall security provides more flexible access control to enforce policies based on user and group identities and the point of access. It also enables simplified policy configuration, so administrators can write policies that correspond to business rules–for increased security, enhanced ease of use, and fewer policies to manage.

What Problems Does It Help Solve?

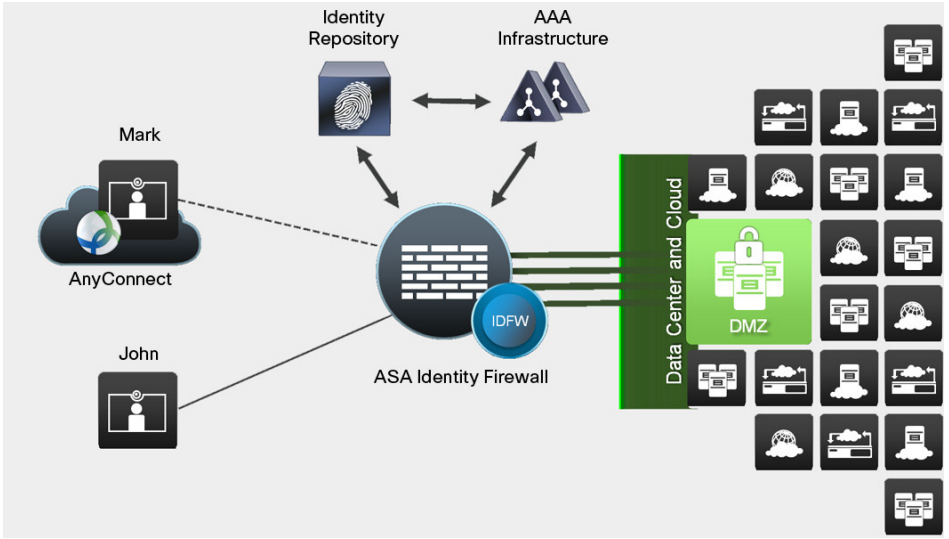
Employees require "anytime, anywhere" access to the network–inside and outside the firewall. Corporate headquarters, branch offices, satellite locations, and VPNs for secure home access all employ different IP addresses. While legacy firewalls require a separate policy for each location to ensure that access can be granted to a specific employee, Cisco identity-based firewall security requires only a single policy: "Allow [Employee ID] access to the network." Similarly, group policies such as "Do not allow marketing to access engineering source code" can be written to provide more precise control over network resources.

What Are the Features of Cisco Identity-Based Firewall Security?

Cisco identity-based firewall security offers advanced features that help reduce costs and operational complexity while increasing overall security. These include:

- **Rich policy language:** Enables effective control of users and groups while reducing the total number of access rules. Policies correspond to business rules, so they are easy to use and to manage. As a result, dramatically fewer policies are required, yet more control is attained. This extensible policy language also integrates with Cisco IPS modules for a comprehensive security solution.
- **Network-agnostic deployment:** Seamlessly integrates with the existing security environment, eliminating the need to change network parameters or install an agent. Once the firewall is deployed, identity-based security is immediately available. There are no conflicts with other policy mechanisms, so existing security policy engines can continue to operate.

Figure 1. Cisco ASA Identity Firewall Deployment

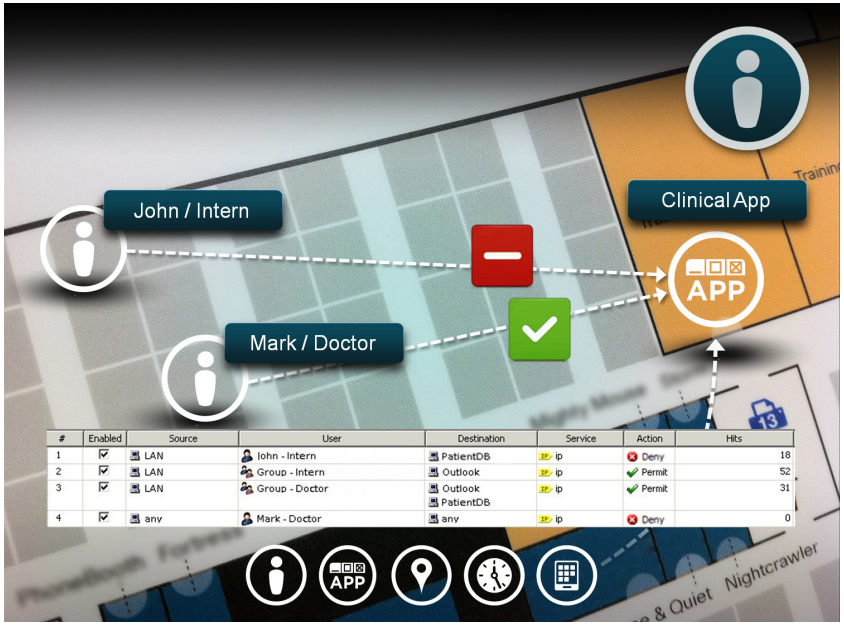


What Are the Benefits?

Cisco identity-based firewall security employs numerous innovations to enable easy and effective control of users and groups while reducing the total number of access rules.

- Identity-based policy enforcement:
  - Aligns policies to user and group rather than IP address
  - Enables policy reconciliation across local and remote users
  - Supports identity-enabled threat control

Figure 2. Cisco ASA Identity Firewall Policy Table



- Flexible deployment options:
  - Can run on a switch or any other endpoint, with no agent required
  - Enables multiple agents to interface with multiple Cisco ASA appliances, to support scalability and high availability needs
  - Interoperates with existing policy mechanisms
  - Agents can be installed on any machine to fit with existing network and security functions
- Simplified policy configuration:
  - IDs can be selected from an existing directory of users and groups, making policies easier to write and more precise to enforce
  - Supports fully qualified domain name (FQDN), so policies can be written using a human-level URL, rather than IP/DNS
  - Integrates with the Cisco ASA family's IPS and content security modules, for easier compliance with IPv6 and regulatory mandates on a per-user/per-group basis.

Why Cisco?

Cisco identity-based firewall security is a component of the Cisco ASA platform, the most widely deployed firewall in the industry. Identity-based security is a critical step toward full context-aware security, which is integral to how the Cisco SecureX Architecture™ meets the evolving security needs of borderless network environments.

Context-aware security provides unparalleled capabilities, enabling organizations to:

- Determine who is trying to access what type of content; the location and time of the attempted access; and the type of application and device being used.
- Correlate both local and global context to provide deeper insight and more effective security.
- Combine in-depth local network context from Cisco TrustSec®,real-time global threat intelligence from Cisco SIO, and unique mobile client insight from Cisco AnyConnect™.
- Provide simplified business policies that correlate directly between what IT must enforce and the organization's business rules.

For More Information

For more information, contact your Cisco account manager or visit one of the following links.

- Cisco ASA 5500 Series Adaptive Security Appliances: http://www.cisco.com/go/asa
- Cisco context-aware security: http://www.cisco.com/en/US/prod/vpndevc/ps6032/ps6094/ps6120/context_aware_security.html
- The Cisco SecureX Architecture: http://www.cisco.com/go/securex

C45-675579-00 06/11