Cisco TrustSec Software-Defined Segmentation

Policy-based approach to simplifying security and reducing risk

Network segmentation is essential for protecting critical business assets. But traditional segmentation approaches are operationally complex. You need to scale the network and still restrict access to critical applications in the data center while improve situational awareness on the network. As the number of roles and endpoints increase within an organization, the cost for managing virtual LANs (VLANs) can be significant. Balancing the demands for agility and security requires a new approach.

Cisco TrustSec® software-defined segmentation dynamically organizes endpoints into logical groups, called security groups. Security groups are assigned based on business decisions using a richer context than an IP address. They are easier for people to understand and manage. And the number of group-based rules is dramatically less than an equivalent set of rules based on IP addresses.

Cisco TrustSec technology is embedded in more than 40 Cisco product families and thirdparty products. It isolates attacks, quickly restricts the lateral movement of threats with micro-segmentation, enables a scalable bring-your-own-device (BYOD) environment, and reduces the scope of compliance for industry and government regulations. A commissioned study conducted by Forrester Consulting on behalf of Cisco now available indicates that customers have found that time-to-implement policy changes can be reduced by 98% and operational costs reduced by as much as 80% with TrustSec software-defined segmentation.

Benefits

- **Limit the impact** of data breaches, compromised devices, and prevent the lateral movement of threats with micro-segmentation

- **Rapid threat containment** to isolate attacks and vulnerable devices

- **Control access to critical enterprise resources** in an easy-to-use matrix

- **Lower operational expenses** through simplified policy management

- **Easily comply with PCI audits** and other compliance requirements

Forrester interviewed customers that had deployed Cisco TrustSec and found:

- **140% Return on investment**
  Composite NPV was $2.33 million. Composite cost to implement was only $1.66 million

- **80% Reduction in IT operational costs**
  Avoid associated costs with operating VLANS and firewalls. Reduce manpower needed to deploy and maintain

- **98% Reduction in time to implement changes**
  Faster time-to-market for projects. Make changes in minutes instead of weeks

Easily control access to your resources

Cisco TrustSec security groups give users access that is consistently maintained as resources move in mobile or virtualized networks. Management at a group-based policy level simplifies switch, router, and firewall rules while still giving you granular control of your network. Want to deny guest tablets on your network? Done. Want to allow tablets for employees in finance? Done.

Decoupling access entitlements from IP addresses and VLANs simplifies security policy and maintenance tasks, lowers operational costs, and allows policies to be consistently applied to wired, wireless, and VPN access.

Policy through the use of security group ACLs (SGACLs) can be dynamically or statically provisioned on switches, routers, and wireless LAN infrastructure. TrustSec segmentation enables security policy to be responsive. It's not just applied when a user enters the network but also responds to how they behave while in the network.

Integration with the Cisco Identity Services Engine

The Cisco® Identity Services Engine (ISE) acts as the controller for software-defined segmentation groups and policies, providing a layer of policy abstraction and centralized administration. Cisco ISE allows segmentation policies to be applied to networks of any size using a simple and clear policy matrix.

Simplifying cross-domain security policy

Cisco ISE is able to share TrustSec group information with other group-based policy schemes used in Cisco's Application-Centric Infrastructure (ACI) and Open Daylight environments to simplify security policy management across domains.

Start protecting your assets today

For more information, please visit: http://www.cisco.com/go/trustsec