Accelerate Group-Based Policy Adoption

Using Cisco Secure Network Analytics' TrustSec Analytics Reporting

Many IT and security professionals that want to pursue policy-based network management find policy adoption challenging for multiple reasons. Some simply don't know how to create the right policies due to a lack of awareness of everything that's running in their environment. Even those who have effectively mapped out their networks often struggle to understand enough about what all their devices are doing to take any action – asking questions like who's talking to who? How are they communicating with one another? Why are they communicating? Are the adhoc policies that are currently in place truly working as intended?

To make matters worse, this lack of visibility into what devices are doing can result in practitioners feeling hesitant to create and implement new policies that could have unintended consequences. For example, by applying a misconfigured policy update, a user could unintentionally allow unauthorized groups to access sensitive information or bring down an entire manufacturing line by restricting operationally critical devices from communicating.

This can result in increased security risks through inaction, as teams end up "stuck", and unable to create and implement the right policies for their environment. All these factors combined ultimately add up to delays in deploying and benefiting from a more secure group-based policy solution.

Security professionals need comprehensive visibility into all devices on their network, what groups are communicating with one another, how they're communicating, and why they're doing so. Deploying Cisco Secure Network Analytics (formerly Stealthwatch) and Cisco Identity Services Engine (ISE) allows practitioners to move beyond these roadblocks via TrustSec-based reports thatenable users to visualize all group communications across an enterprise's network in order to adopt the right policies and adapt them to the needs of their environment.



© 2021 Cisco and/or its affiliates. All rights reserved.

Tightly coupling Cisco Secure Network Analytics and Cisco Identity Services Engine significantly enhances group-based policy visibility, enabling users to:

- Observe more inter-group communications effortlessly by visualizing what groups within their environment are communicating with one another via TrustSec Analytics reports that map group communications between up to 250 Security Group Tags (SGTs).
- Validate the efficacy of policies by examining near real-time network telemetry flows between groups to monitor whether trusted ISE policies are being observed as intended and adapt them when necessary.
- Streamline policy violation investigations by generating TrustSec Policy Analytics reports which provide granular insights into all relevant flows between SGTs and associated IPs to enable quick and effective responses to policy violations.
- Analyze changes in traffic patterns with TrustSec reporting data that is retained for 30 days across all SGTs to better understand how policy changes have impacted network telemetry flows over time.

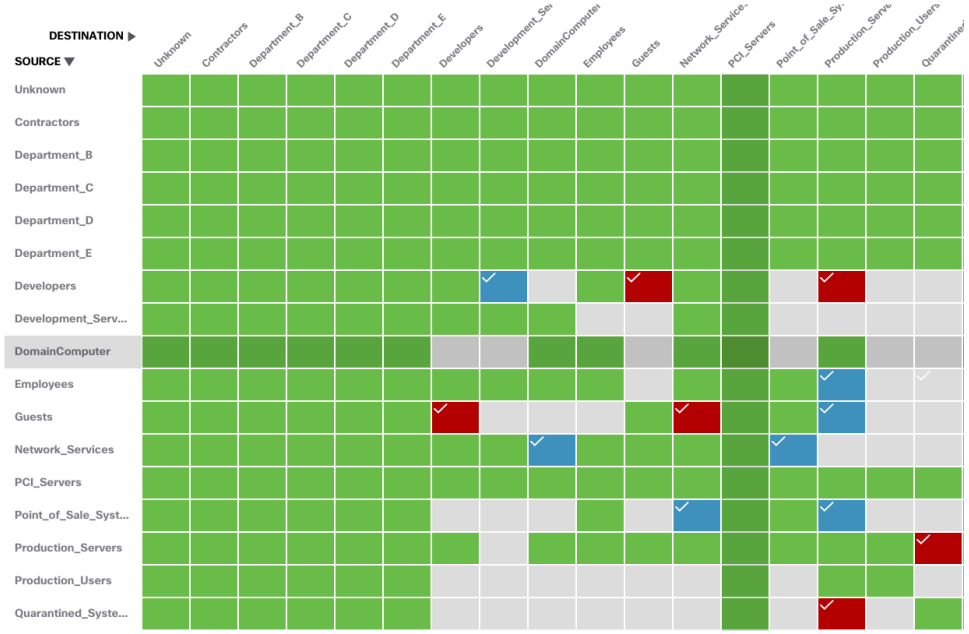
IT and security teams that want to adopt group-based policies can do so by leveraging pre-existing Cisco infrastructure investments that support SGTs such as Catalyst Switches, Integrated Services Routers, Aggregation Services Routers, and more. Learn more about the TrustSec Matrix and all SGT-supported Cisco TrustSec devices here.



© 2021 Cisco and/or its affiliates. All rights reserved.

TrustSec Analytics Report

A TrustSec Analytics report generated in Secure Network Analytics that displays volumetric communications between different SGTs that have been assigned and pulled directly from ISE.



© 2021 Cisco and/or its affiliates. All rights reserved.

Visualize group communications between Security Group Tags with the Cisco TrustSec Matrix

Group-Based Policies use labels called Security Group Tags (SGTs) to represent logical groupings of users and/or devices. SGTs are applied by Cisco Identity Services Engine (ISE) as entities request access to the network. As these users and devices communicate across the network, telemetry that includes the SGTs can be sent to Secure Network Analytics. The Report Builder application can then be used to create TrustSec Analytics reports which map communications between SGTs, allowing users to visualize all communications between the different groups within their environment.

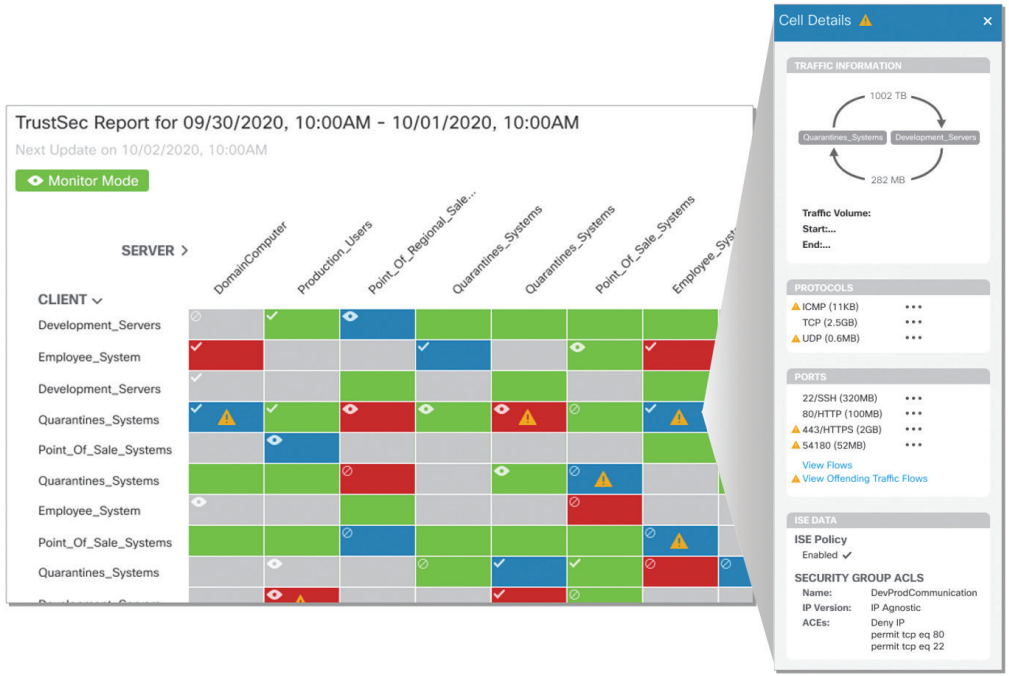
Validate whether trusted ISE policies are being observed via real-time network telemetry.

Once groups have been properly established, the next step in group-based policy adoption is the creation and monitoring of policies. The TrustSec Policy Analytics report can also be generated through Secure Network Analytics' Report Builder application to provide a more granular view into the communication patterns between SGTs to allow users to determine whether trusted ISE policies are being observed or violated.

Users can drill down further on the communication patterns between any two groups by clicking on a cell in the report to bring up a side panel that not only includes details on the volume of data being sent between the two groups, but also provides visibility into how that data is being distributed and whether it appears to violate the policy. The side panel also includes information on the types protocols being used, what ports they are operating on, and the associated ISE policy.

TrustSec Policy Analytics Report

A TrustSec Policy Analytics report generated in Secure Network Analytics with intuitive color-coded cells and labels that indicate whether communications between different SGTs are violating a policy and require further investigation.



© 2021 Cisco and/or its affiliates. All rights reserved.

Additionally, when it comes to the typically lengthy processes associated with determining a policy violation's root cause, the capabilities offered by the TrustSec Policy Analytics report quite literally enable users to find the proverbial 'offending-flow needles' in their vast 'network haystacks'. When a user clicks on a cell displaying a policy violation, a nearly identical side panel as described above will appear, but that also offers users the ability to drill down even further via the linked option to "View Offending Traffic Flows". Rather than performing hours upon hours of cumbersome tasks such as conducting manual searches and cross-references across different datasets, users can click this link to generate another report based of off all the associated IPs and related flows observed by Secure Network Analytics. This provides immediate insights into all associated endpoints, ISE-registered usernames, and events with timestamps on single pane, effectively allowing users to streamline their root cause analysis efforts and expedite their ability to diagnose why a policy violation occurred.



Summary

Secure Network Analytics' TrustSec reports lower the entry point to pursuing group-based policy management by allowing practitioners to visualize inter-group communications within their networks, analyze whether those communications comply with ISE-based policies, and identify communications that have been observed as non-compliant. These reports provide quick lines to further investigate possible violations and to gain insights into their communication patterns and why groups are communicating. This enables practitioners to adopt new policies, adapt them to their organization's needs through ISE, and continuously monitor their efficacy. By facilitating policy adoption efforts, the TrustSec reports essentially allows users to achieve the benefits of intent-based networking immediately via their existing Cisco architecture, while also positioning them for future software-defined access adoption.

Next Steps

To learn more about Secure Network Analytics, visit:

https://www.cisco.com/go/secure-network-analytics

To learn more about Identity Services Engine, visit:

https://www.cisco.com/go/ise

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. 2307844 01/21