Cisco Stealthwatch Proxy Integration Service

Benefits

- Integrates proxy records from your proxy server into most any database, such as an SQL or Hadoop database. Query the database to retrieve and analyze desired data, which will help orient security teams to potentially malicious external sites.
- View the communication from the internal host to the proxy and out to the external URL, providing 100% visibility into user activity on the network.
- Query Cisco® Stealthwatch to see how many internal hosts are visiting potentially malicious external URLs and identify who the users are, when they visited a site and how much, if any, data was sent or received, which reduces data loss and infection from harmful sites.
- Security teams are alerted to unacceptable network use based on the URL or domain visited, which helps mitigate corporate policy violations. This helps you maintain a more secure network and remain in compliance.
- Perform quick and accurate forensic investigation of command and control communications across the proxy server to improve your overall security posture.

Proxy Server Integration Provides Granular Visibility and Context

Use the Cisco Stealthwatch Proxy Integration Service to integrate virtually any web proxy with the Cisco Stealthwatch Flow Collector and extend network visibility between internal hosts, across proxy servers, and out to the public Internet and public web services. This end-to-end network visibility spans web proxies, and expands network protection, improves threat detection, and reduces your corporate risk with the granular visibility afforded by the integration service. The Proxy Integration Service gives offers deep integration of any proxy server into your network for more detailed queries into command and control activity, potentially malicious host and customized alerting. This custom designed integration service fully leverages the capabilities and data provided by your proxy servers.

By taking advantage of our team of experts, you can optimize Stealthwatch's operations and promote successful integration with your internal business policies. The services provide enhanced security intelligence, optimized network performance, and increased return on investment.

The integration of Cisco Stealthwatch with your web proxy servers adds an additional layer of context, protection, and security to your overall posture.

Our Cisco Stealthwatch Proxy Integration Service consists of a proxy adapter component and the services required to integrate your web proxy with a Cisco Stealthwatch Flow Collector. The proxy adapter listens for incoming syslog messages, then converts them to NetFlow records that are sent to a flow collector. The adapter gives visibility into web traffic that traverses the proxy by providing application details that include the URL and domain information, which provides in-depth details on who is visiting what web service and when they visited.

The adapter runs on a virtual machine or physical server and converts proxy syslog messages to NetFlow for analysis by a flow collector. You can:

- Integrate your web proxy with the Stealthwatch Flow Collector to extend network visibility into stitched flows between internal clients and outside web servers to improve your visibility to the outside Internet.
- Gain piece of mind by having visibility into who is accessing the proxy and what URLs are being visited.
- Seamlessly integrate with supported proxy servers for visibility of data in the flow collectors.
- Customize and integrate with virtually every proxy server available for maximum flexibility.
- Ensure that all Internet-bound traffic is using the proxy as defined by corporate policy to prevent policy violations.

Professional services will spend five days with your team completing the integrations. The service can be delivered either in-person or through virtual sessions, and includes the integration for up to four proxy servers. Upon completion of the service, there will be a knowledge transfer session, and all documentation on how the service was performed will be provided so the security team can perform future integration.

The Cisco Security Stealthwatch Proxy Integration Service can enable you to achieve end-to-end network visibility that spans web proxies. This expands your network protection and increases your return on investment of your Stealthwatch deployment so that your organization is more aware of proxy traffic. The result is a safer, more resilient network.

Next Steps

To learn more about Cisco Security Services and how our Stealthwatch deployment services can benefit your business, contact your local account representative or authorized Cisco reseller. For more information on how Cisco can help you protect your organization from today's dynamic threats, visit www.cisco.com/go/services/security.

C45-736853-00 05/16