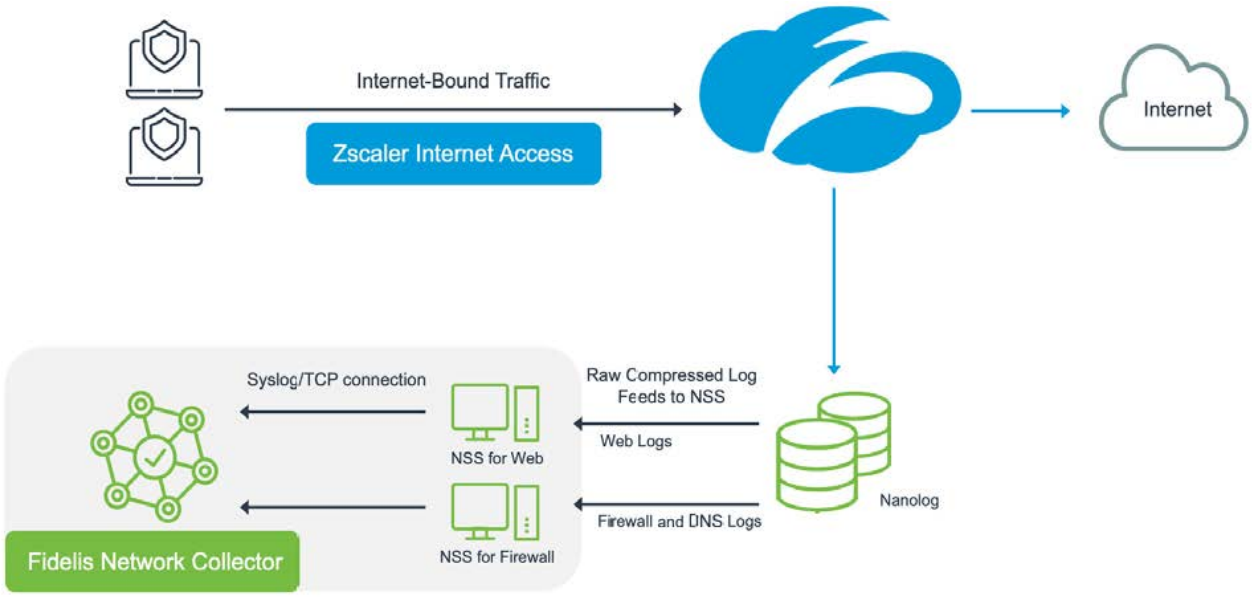
DEPLOYMENT GUIDE

Fidelis Network and Zscaler Internet Access

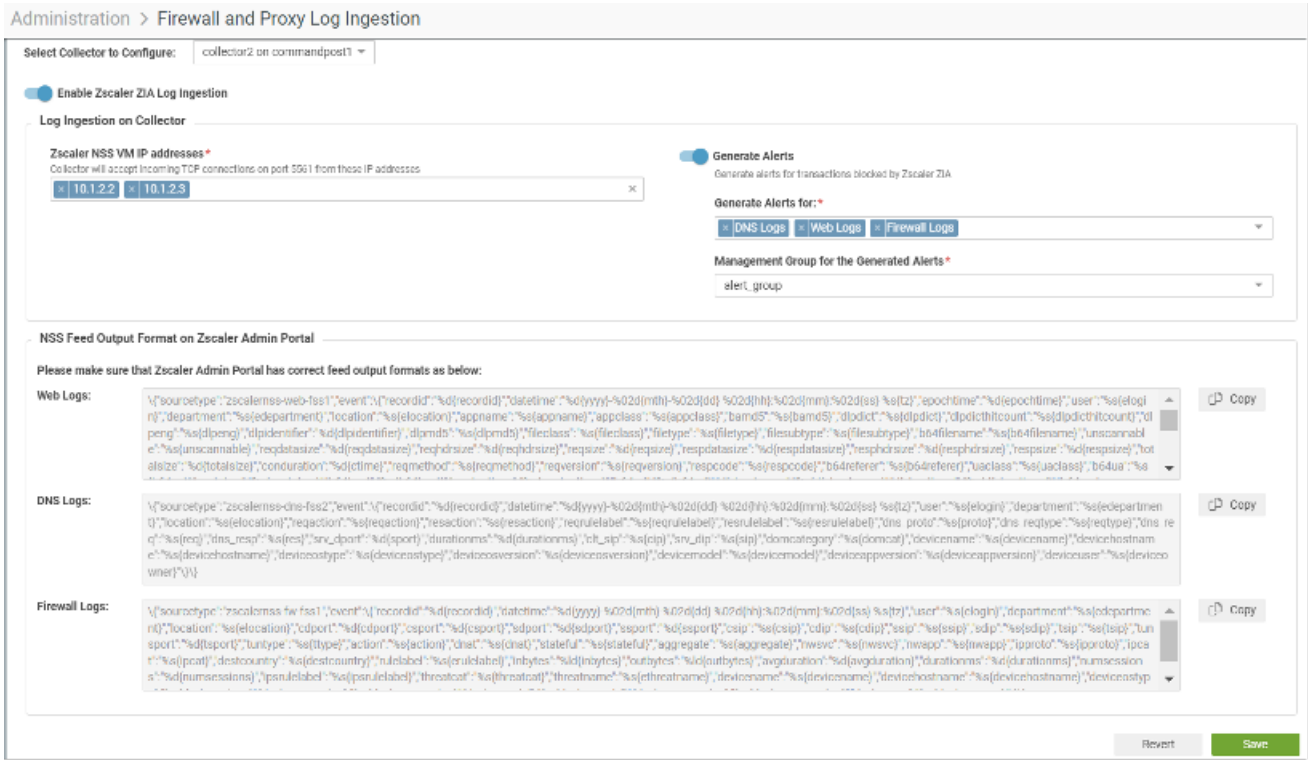
This guide provides high-level information on the integrated deployment of Fidelis Network® and Zscaler Internet Access (ZIA) products. The use cases and joint value of the solution are covered in “Joint Solution Guide” [1], and the details on configuring the products are covered in the “User’s Guide” for Fidelis Network [2].

The integration between Fidelis Network and Zscaler Internet Access (ZIA) is available with Fidelis Network version 9.5 and requires the use of Zscaler NSS (Nanolog Streaming Service) [3]. NSS can be installed as a VM within the same subnet where the Fidelis Network Collector is connected. The NSS VM receives the ZIA logs from Zscaler Cloud over a TLS encrypted channel and forwards them to the Fidelis Network Collector product over TCP (unencrypted) as in the figure below:

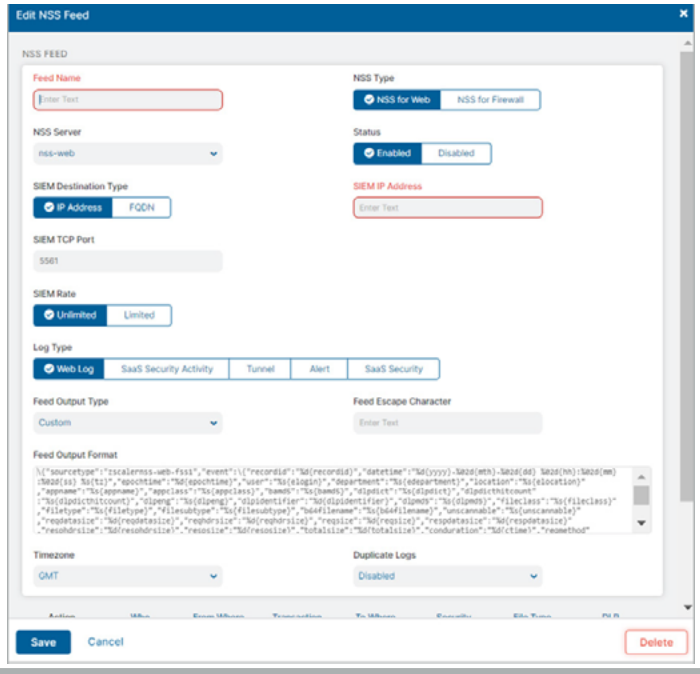


For remote clients that use Zscaler Client Connector, Z-Tunnel 2.0 is highly recommended, and is required for collecting Firewall and DNS logs from NSS. To configure the deployment, the following steps should be followed. More details for each step can be found in [2] and [3].

1. **ZIA Admin Portal**
   Monitor the peak transaction count for the traffic in Zscaler whose logs would be sent to Fidelis Network.
2. **ZIA Admin Portal**
   Provision the NSS Servers for both Firewall and Web traffic in the ZIA portal. The NSS Servers should be provisioned adjacent to the Fidelis Network Collectors in IP space, in the same network subnet. Confirm that the servers are enabled and healthy. For Fidelis Network SaaS Cloud deployments, contact Fidelis Support for this step.
3. **Fidelis Network**
   Enable Zscaler ZIA log ingestion on the 'Administration - Firewall and Proxy Log Ingestion' page of the Fidelis CommandPost. Specify the NSS VM IP address(es), and whether to display ZIA blocked transactions as alerts. The output format for each NSS log type is available directly from this page for copy and paste into the NSS feed definitions in step 4.

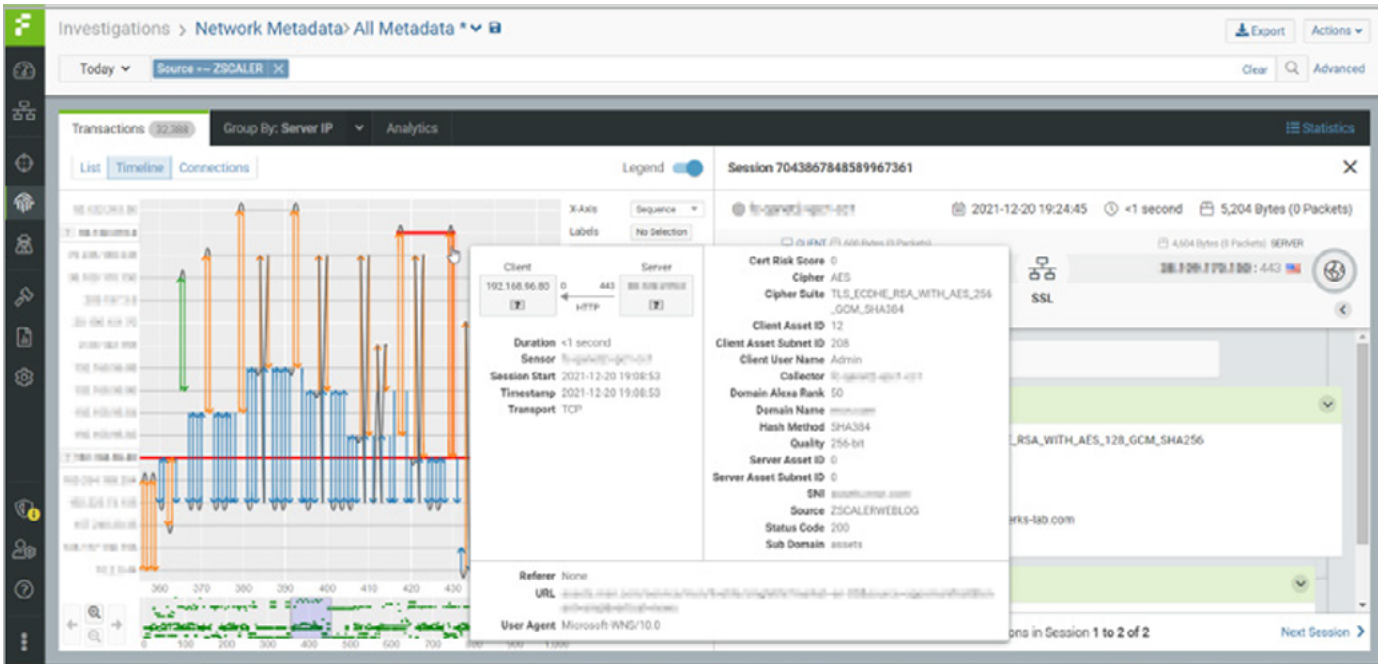


4. **ZIA Admin Portal**
   Configure ZIA to create NSS feeds [4] [5] [6] and start the flow of logs from the NSS VM to Fidelis Network Collector. The 'SIEM IP Address' field should be the IP address of the Fidelis Network Collector, and the 'SIEM TCP Port' should be 5561. The specific "Feed Output Format" as well as other recommended fields for Fidelis Network are in Appendix A as well as the Fidelis Network User's Guide [2] which is available as context sensitive help in Fidelis GUI.



5. Fidelis Network Collector

Test the integration by logging into Fidelis CommandPost, searching All Metadata for “Source =~ Zscaler” and verify that logs are being ingested as transactions in the screenshot below.



References

[1] “Fidelis Network – Zscaler Internet Access Joint: Joint Solution Brief”, Fidelis Cybersecurity.
[2] “Fidelis Network User’s Guide: version 9.5 and later”, Fidelis Cybersecurity.
[3] “About Nanolog Streaming Service”, Zscaler Help page. https://help.zscaler.com/zia/about-nanolog-streaming-service
[4] “Adding NSS Feeds for Web Logs”, Zscaler Help page. https://help.zscaler.com/zia/adding-nss-feeds-web-logs
[5] “Adding NSS Feeds for Firewall Logs”, Zscaler Help page. https://help.zscaler.com/zia/adding-nss-feeds-firewall-logs
[6] “Adding NSS Feeds for DNS Logs”, Zscaler Help page. https://help.zscaler.com/zia/adding-nss-feeds-dns-logs

Appendix A: NSS Feed Configuration Field

In NSS Feed creation, the following configuration should be followed:

‘SIEM Rate’ should be Unlimited

‘Log Type’ should be
- **‘Web Log’** for Web Feed
- **‘Firewall Logs’** for Firewall Feed
- **‘DNS Logs’** for DNS Feed

‘Feed Output Type’ should be **‘Custom’**

‘Feed Escape Character’ should be empty

‘Timezone’ should be GMT

‘Duplicate Logs’ should be disabled

The **‘Feed Output Format’** for different feeds should be copy pasted from strings below (no newlines):
- Web Feed

```
\{"sourcetype":"zscalernss-web-fss1","event":\{"recordid":"%d{recordid}","datetime":"%d{yyyy}-
%02d{mth}-%02d{dd} %02d{hh}:%02d{mm}:%02d{ss}
%s{tz}","epochtime":"%d{epochtime}","user":"%s{elogin}","department":"%s{edepartment}","location":"%s{elocation}",
"appname":"%s{appname}","appclass":"%s{appclass}","bamd5":"%s{bamd5}","dlpdict":"%s{dlpdict}",
"dlpdicthitcount":"%s{dlpdicthitcount}","dlpeng":"%s{dlpeng}","dlpidentifier":"%d{dlpidentifier}","dlpmd5":"%s{dlpmd5}",
"fileclass":"%s{fileclass}","filetype":"%s{filetype}","filesubtype":"%s{filesubtype}","b64filename":"%s{b64filename}",
"unscannable":"%s{unscannable}","reqdatasize":"%d{reqdatasize}","reqhdrsize":"%d{reqhdrsize}","reqsize":"%d{reqsize}",
"respdatasize":"%d{respdatasize}","resphdrsize":"%d{resphdrsize}","respsize":"%d{respsize}","totalsize":"%d{totalsize}",
"conduration":"%d{ctime}","reqmethod":"%s{reqmethod}","reqversion":"%s{reqversion}","respcode":"%s{respcode}",
"b64referer":"%s{b64referer}","uaclass":"%s{uaclass}","b64ua":"%s{b64ua}","ua_token":"%s{ua_token}","b64host":"%s{b64host}",
"contenttype":"%s{contenttype}","b64url":"%s{b64url}","df_hostname":"%s{df_hostname}","df_hosthead":"%s{df_hosthead}",
"b64mobappname":"%s{b64mobappname}","mobappcat":"%s{mobappcat}","mobdevtype":"%s{mobdevtype}","cip":"%s{cip}",
"cintip":"%s{cintip}","cltipv6":"%s{cltipv6}","sip":"%s{sip}","appproto":"%s{proto}","b64rulelabel":"%s{b64rulelabel}",
"ruletype":"%s{ruletype}","reason":"%s{reason}","action":"%s{action}","b64urlfilterrulelabel":"%s{b64urlfilterrulelabel}",
"b64apprulelabel":"%s{b64apprulelabel}","ssldecrypted":"%s{ssldecrypted}","clientsslcipher":"%s{clientsslcipher}",
"clienttlsversion":"%s{clienttlsversion}","clientsslsessreuse":"%s{clientsslsessreuse}","srvsslcipher":"%s{srvsslcipher}",
"srvtlsversion":"%s{srvtlsversion}","srvocspresult":"%s{srvocspresult}","srvcertchainvalpass":"%s{srvcertchainvalpass}",
"srvwildcardcert":"%s{srvwildcardcert}","serversslsessreuse":"%s{serversslsessreuse}","srvcertvalidationtype":"%s{srvcertvalidationtype}",
"srvcertvalidityperiod":"%s{srvcertvalidityperiod}","riskscore":"%d{riskscore}","b64threatname":"%s{b64threatname}",
"malwareclass":"%s{malwareclass}","malwarecat":"%s{malwarecat}","urlclass":"%s{urlclass}","urlsupercat":"%s{urlsupercat}",
"b64urlcat":"%s{b64urlcat}","trafficredirectmethod":"%s{trafficredirectmethod}","ztunnelversion":"%s{ztunnelversion}",
"productversion":"%s{productversion}","devicename":"%s{devicename}","devicehostname":"%s{devicehostname}",
"deviceostype":"%s{deviceostype}","deviceosversion":"%s{deviceosversion}","devicemodel":"%s{devicemodel}",
"deviceappversion":"%s{deviceappversion}","deviceuser":"%s{deviceowner}"\}\}
```

- Firewall Feed

\{"sourcetype":"zscalernss-fw-fss1","event":\{"recordid":"%d{recordid}",
"datetime":"%d{yyyy}-%02d{mth}-%02d{dd} %02d{hh}:%02d{mm}:%02d{ss}
%s{tz}","user":"%s{elogin}","department":"%s{edepartment}","location":"%s{elocation}","cdport":"%d{cdport}","csport":"%d{csport}",
"sdport":"%d{sdport}","ssport":"%d{ssport}","csip":"%s{csip}","cdip":"%s{cdip}","ssip":"%s{ssip}","sdip":"%s{sdip}","tsip":"%s{tsip}",
"tunsport":"%d{tsport}","tuntype":"%s{ttype}","action":"%s{action}","dnat":"%s{dnat}","stateful":"%s{stateful}","aggregate":"%s{aggregate}",
"nwsvc":"%s{nwsvc}","nwapp":"%s{nwapp}","ipproto":"%s{ipproto}","ipcat":"%s{ipcat}","destcountry":"%s{destcountry}",
"rulelabel":"%s{erulelabel}","inbytes":"%ld{inbytes}","outbytes":"%ld{outbytes}","avgduration":"%d{avgduration}",
"durationms":"%d{durationms}","numsessions":"%d{numsessions}","ipsrulelabel":"%s{ipsrulelabel}","threatcat":"%s{threatcat}",
"threatname":"%s{ethreatname}","devicename":"%s{devicename}","devicehostname":"%s{devicehostname}","deviceostype":"%s{deviceos-
type}",
"deviceosversion":"%s{deviceosversion}","devicemodel":"%s{devicemodel}","deviceappversion":"%s{deviceappversion}",
"deviceuser":"%s{deviceowner}"\}\}

- DNS Feed

\{"sourcetype":"zscalernss-dns-fss2","event":\{"recordid":"%d{recordid}",
"datetime":"%d{yyyy}-%02d{mth}-%02d{dd} %02d{hh}:%02d{mm}:%02d{ss} %s{tz}","user":"%s{elogin}",
"department":"%s{edepartment}","location":"%s{elocation}","reqaction":"%s{reqaction}","resaction":"%s{resaction}",
"reqrulelabel":"%s{reqrulelabel}","resrulelabel":"%s{resrulelabel}","dns_proto":"%s{proto}","dns_reqtype":"%s{reqtype}",
"dns_req":"%s{req}","dns_resp":"%s{res}","srv_dport":"%d{sport}","durationms":"%d{durationms}","clt_sip":"%s{cip}","srv_dip":"%s{sip}",
"domcategory":"%s{domcat}","devicename":"%s{devicename}","devicehostname":"%s{devicehostname}","deviceostype":"%s{deviceostype}",
"deviceosversion":"%s{deviceosversion}","devicemodel":"%s{devicemodel}","deviceappversion":"%s{deviceappversion}",
"deviceuser":"%s{deviceowner}"\}\}

For more information, please contact
Fidelis Cybersecurity Technical Support at

support@fidelissecurity.com or **1.800.652.4020**

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

About Fidelis Cybersecurity

Fidelis Cybersecurity, the industry innovator in Active XDR and proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via deep, dynamic asset discovery, multi-faceted context, and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. Fidelis Cybersecurity is dedicated to helping clients become stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit **www.fidelissecurity.com**