```
[2232:root:3]allocSSLConn:297 sconn 0x7ffa19d99e00 (0:root)
[2232:root:3]SSL state:before SSL initialization (10.5.27.2)
[2232:root:3]SSL state:before SSL initialization (10.5.27.2)
[2232:root:3]client cert requirement: no
[2232:root:3]SSL state:SSLv3/TLS read client hello (10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS write server hello (10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS write certificate (10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS write key exchange (10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS write server done (10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS write server done:system lib(10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS write server done (10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS read client key exchange (10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS read change cipher spec (10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS read finished (10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS write session ticket (10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS write change cipher spec (10.5.27.2)
[2232:root:3]SSL state:SSLv3/TLS write finished (10.5.27.2)
[2232:root:3]SSL state:SSL negotiation finished successfully (10.5.27.2)
[2232:root:3]SSL established: TLSv1.2 DHE-RSA-AES256-GCM-SHA384
[2232:root:3]req: /
[2232:root:3]mza: 0x2a63ec0 /rmt_index.html
[2232:root:3]def: 0x2a63ec0 /rmt_index.html
[2232:root:3]req: /remote/info
[2232:root:3]capability flags: 0xdf
[2232:root:3]req: /remote/login
[2232:root:3]rmt_web_auth_info_parser_common:468 no session id in auth
info
[2232:root:3]rmt_web_get_access_cache:820 invalid cache, ret=4103
[2232:root:3]User Agent: FortiSSLVPN (Windows NT; SV1 [SV{v=02.01;
f=07;}])
[2232:root:3]get_cust_page:128 saml_info 0
[2232:root:3]req: /remote/logincheck
[2232:root:3]rmt_web_auth_info_parser_common:468 no session id in auth
info
[2232:root:3]rmt_web_access_check:739 access failed,
uri=[/remote/logincheck],ret=4103,
[2232:root:3]User Agent: FortiSSLVPN (Windows NT; SV1 [SV{v=02.01;
f=07;}])
[2232:root:3]rmt_logincheck_cb_handler:1285 user 'prateek' has a matched
local entry.
[2232:root:3]sslvpn_auth_check_usrgroup:2635 forming user/group list from
policy.
[2232:root:3]sslvpn_auth_check_usrgroup:2673 got user (2) group (1:0).
[2232:root:3]sslvpn_validate_user_group_list:1825 validating with SSL VPN
authentication rules (1), realm ().
[2232:root:3]sslvpn_validate_user_group_list:1906 checking rule 1 cipher.
[2232:root:3]sslvpn_validate_user_group_list:1914 checking rule 1 realm.
[2232:root:3]sslvpn_validate_user_group_list:1925 checking rule 1 source
intf.
[2232:root:3]sslvpn_validate_user_group_list:1964 checking rule 1 vd
source intf.
[2232:root:3]sslvpn_validate_user_group_list:2210 rule 1 done, got user
(0:0) group (1:0) peer group (0).
[2232:root:3]sslvpn_validate_user_group_list:2538 got user (2:0), group
(1:0) peer group (0).
[2232:root:3]sslvpn_update_user_group_list:1771 got user (2:0), group
(1:0), peer group (0) after update.
[2232:root:3]two factor check for prateek: off
```

```
[2232:root:3]sslvpn_authenticate_user:166 authenticate user: [prateek]
[2232:root:3]sslvpn_authenticate_user:173 create fam state
[2232:root:3]fam_auth_send_req:880 found node prateek:0:, valid:1
[2232:root:3][fam_auth_send_req_internal:424] Groups sent to FNBAM:
[2232:root:3]group_desc[0].grpname = prateek
[2232:root:3]group_desc[1].grpname = Domain Group
[2232:root:3][fam_auth_send_req_internal:436] FNBAM opt = 0X201420
[1909] handle_req-Rcvd auth req 1682345159 for prateek in  opt=00201420
prot=11
[466] __compose_group_list_from_req-Group 'prateek', type 5
[466] __compose_group_list_from_req-Group 'Domain Group', type 1
[617] fnbamd_pop3_start-prateek
[380] radius_start-Didn't find radius servers (0)
[750] auth_tac_plus_start-Didn't find tac_plus servers (0)
[954] __fnbamd_cfg_get_ldap_list_by_user-
[2147] __match_and_update_auth_user-Found a matching user in CMDB
'prateek'
[942] __fnbamd_cfg_add_ldap_by_user-Loaded LDAP server 'My-LDAP' for user
'prateek' (16777218)
[2232:root:3]fam_auth_send_req_internal:512 fnbam_auth return: 4
[1131] fnbamd_cfg_get_ldap_list-Total ldap servers to try: 1
[1713] fnbamd_ldap_init-search filter is: sAMAccountName=prateek
[1722] fnbamd_ldap_init-search base is: DC=SISCO,DC=COM
[1146] __fnbamd_ldap_dns_cb-Resolved My-LDAP:10.220.6.107 to
10.220.6.107, cur stack size:1
[919] __fnbamd_ldap_get_next_addr-
[1152] __fnbamd_ldap_dns_cb-Connection starts My-LDAP:10.220.6.107, addr
10.220.6.107 over SSL
[874] __fnbamd_ldap_start_conn-Still connecting 10.220.6.107.
[633] create_auth_session-Total 1 server(s) to try
[1103] __ldap_connect-tcps_connect(10.220.6.107) is established.
[981] __ldap_rxtx-state 3(Admin Binding)
[363] __ldap_build_bind_req-Binding to 'sisco\administrator'
[1084] fnbamd_ldap_send-sending 43 bytes to 10.220.6.107
[1096] fnbamd_ldap_send-Request is sent. ID 1
[981] __ldap_rxtx-state 4(Admin Bind resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
[1307] fnbamd_ldap_recv-Response len: 16, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:1, type:bind
[1023] fnbamd_ldap_parse_response-ret=0
[1048] __ldap_rxtx-Change state to 'DN search'
[981] __ldap_rxtx-state 11(DN search)
[751] fnbamd_ldap_build_dn_search_req-base:'DC=SISCO,DC=COM'
filter:sAMAccountName=prateek
[1084] fnbamd_ldap_send-sending 73 bytes to 10.220.6.107
[1096] fnbamd_ldap_send-Request is sent. ID 2
[981] __ldap_rxtx-state 12(DN search resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 50
[1307] fnbamd_ldap_recv-Response len: 52, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-entry
[1023] fnbamd_ldap_parse_response-ret=0
[1220] __fnbamd_ldap_dn_entry-Get DN
'CN=prateek,CN=Users,DC=SISCO,DC=com'
[1127] __fnbamd_ldap_read-Read 8
```

```
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 63
[1307] fnbamd_ldap_recv-Response len: 65, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-
reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 75
[1307] fnbamd_ldap_recv-Response len: 77, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-
reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 75
[1307] fnbamd_ldap_recv-Response len: 77, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-
reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 59
[1307] fnbamd_ldap_recv-Response len: 61, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-
reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
[1307] fnbamd_ldap_recv-Response len: 16, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-
result
[1023] fnbamd_ldap_parse_response-ret=0
[1048] __ldap_rxtx-Change state to 'User Binding'
[981] __ldap_rxtx-state 5(User Binding)
[596] fnbamd_ldap_build_userbind_req-Trying DN
'CN=prateek,CN=Users,DC=SISCO,DC=com'
[363] __ldap_build_bind_req-Binding to
'CN=prateek,CN=Users,DC=SISCO,DC=com'
[1084] fnbamd_ldap_send-sending 88 bytes to 10.220.6.107
[1096] fnbamd_ldap_send-Request is sent. ID 3
[981] __ldap_rxtx-state 6(User Bind resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
[1307] fnbamd_ldap_recv-Response len: 16, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:3, type:bind
[1023] fnbamd_ldap_parse_response-ret=0
[1048] __ldap_rxtx-Change state to 'Attr query'
[981] __ldap_rxtx-state 7(Attr query)
[649] fnbamd_ldap_build_attr_search_req-Adding attr 'memberOf'
[661] fnbamd_ldap_build_attr_search_req-
base:'CN=prateek,CN=Users,DC=SISCO,DC=com' filter:cn=*
[1084] fnbamd_ldap_send-sending 111 bytes to 10.220.6.107
[1096] fnbamd_ldap_send-Request is sent. ID 4
[981] __ldap_rxtx-state 8(Attr query resp)
[1127] __fnbamd_ldap_read-Read 8
```

```
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 244
[1307] fnbamd_ldap_recv-Response len: 246, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:4, type:search-entry
[1023] fnbamd_ldap_parse_response-ret=0
[556] __get_member_of_groups-Get the memberOf groups.
[522] __retrieve_group_values-Get the memberOf groups.
[533] __retrieve_group_values- attr='memberOf', found 2 values
[542] __retrieve_group_values-
val[0]='CN=Restricted,CN=Users,DC=SISCO,DC=com'
[542] __retrieve_group_values-val[1]='CN=Domain
Computers,CN=Users,DC=SISCO,DC=com'
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
[1307] fnbamd_ldap_recv-Response len: 16, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:4, type:search-
result
[1023] fnbamd_ldap_parse_response-ret=0
[1300] __fnbamd_ldap_attr_next-Entering CHKPRIMARYGRP state
[1048] __ldap_rxtx-Change state to 'Primary group query'
[981] __ldap_rxtx-state 13(Primary group query)
[685] fnbamd_ldap_build_primary_grp_search_req-starting primary group
check...
[689] fnbamd_ldap_build_primary_grp_search_req-number of sub auths 5
[707] fnbamd_ldap_build_primary_grp_search_req-base:'DC=SISCO,DC=COM'
filter:(&(objectclass=group)(objectSid=\01\05\00\00\00\00\00\05\15\00\00\
00\7b\81\97\ee\75\c2\44\96\78\f6\8d\96\01\02\00\00))
[1084] fnbamd_ldap_send-sending 119 bytes to 10.220.6.107
[1096] fnbamd_ldap_send-Request is sent. ID 5
[981] __ldap_rxtx-state 14(Primary group query resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 108
[1307] fnbamd_ldap_recv-Response len: 110, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-entry
[1023] fnbamd_ldap_parse_response-ret=0
[472] __get_one_group-group: CN=Domain Users,CN=Users,DC=SISCO,DC=com
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 63
[1307] fnbamd_ldap_recv-Response len: 65, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-
reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 75
[1307] fnbamd_ldap_recv-Response len: 77, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-
reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 75
[1307] fnbamd_ldap_recv-Response len: 77, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-
reference
```

```
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 59
[1307] fnbamd_ldap_recv-Response len: 61, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-
reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
[1307] fnbamd_ldap_recv-Response len: 16, svr: 10.220.6.107
[988] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-
result
[1023] fnbamd_ldap_parse_response-ret=0
[1428] __fnbamd_ldap_primary_grp_next-Auth accepted
[1048] __ldap_rxtx-Change state to 'Done'
[981] __ldap_rxtx-state 23(Done)
[1084] fnbamd_ldap_send-sending 7 bytes to 10.220.6.107
[1096] fnbamd_ldap_send-Request is sent. ID 6
[785] __ldap_done-svr 'My-LDAP'
[755] __ldap_destroy-
[725] __ldap_stop-Conn with 10.220.6.107 destroyed.
[2679] fnbamd_ldap_result-Result for ldap svr 10.220.6.107(My-LDAP) is
SUCCESS
[401] ldap_copy_grp_list-copied CN=Restricted,CN=Users,DC=SISCO,DC=com
[401] ldap_copy_grp_list-copied CN=Domain
Computers,CN=Users,DC=SISCO,DC=com
[401] ldap_copy_grp_list-copied CN=Domain Users,CN=Users,DC=SISCO,DC=com
[1636] fnbam_user_auth_group_match-req id: 1682345159, server: My-LDAP,
local auth: 0, dn match: 1
[1582] __group_match-User 'prateek' passed group matching
[1585] __group_match-Add matched user 'prateek'(16777218)
[1603] __group_match-Group 'Domain Group' passed group matching
[1606] __group_match-Add matched group 'Domain Group'(2)
[2690] fnbamd_ldap_result-Passed group matching
[217] fnbamd_comm_send_result-Sending result 0 (nid 0) for req
1682345159, len=2214
[2232:root:3]fam_auth_proc_resp:1294 fnbam_auth_update_result return: 0
[2232:root:3][fam_auth_proc_resp:1392] Authenticated groups (2) by FNBAM
with auth_type (16):
[2232:root:3][789] destroy_auth_session-delete session 1682345159
[755] __ldap_destroy-
[1764] fnbamd_ldap_auth_ctx_free-Freeing 'My-LDAP' ctx
Received: auth_rsp_data.grp_list[0] = 16777218
[2232:root:3]Received: auth_rsp_data.grp_list[1] = 2
[2232:root:3]fam_auth_proc_resp:1417 found node Domain Group:0:, valid:1,
auth:0
[2232:root:3]Validated: auth_rsp_data.grp_list[1] = Domain Group
[2232:root:3]Auth successful for user prateek
[2232:root:3]fam_do_cb:663 fnbamd return auth success.
[2232:root:3]SSL VPN login matched rule (0).
[2232:root:3]got public IP address: X.X.X.X
[2232:root:3]User Agent: FortiSSLVPN (Windows NT; SV1 [SV{v=02.01;
f=07;}])
[2232:root:3]rmt_web_session_create:1144 create web session, idx[0]
[2232:root:3]login_succeeded:534 redirect to hostcheck
```

```
[2232:root:3]User Agent: FortiSSLVPN (Windows NT; SV1 [SV{v=02.01;
f=07;}])
[2232:root:3]deconstruct_session_id:694 decode session id ok,
user=[prateek], group=[],authserver=[My-LDAP],portal=[web-
access],host[10.5.27.2],realm=[],csrf_token=[6254EE3AC06AF4B53A89C123D215
C7],idx=0,auth=16,sid=38b70ccb,login=1638168992,access=1638168992,saml_lo
gout_url=no,pip=X.X.X.X
[2232:root:3]deconstruct_session_id:694 decode session id ok,
user=[prateek], group=[],authserver=[My-LDAP],portal=[web-
access],host[10.5.27.2],realm=[],csrf_token=[6254EE3AC06AF4B53A89C123D215
C7],idx=0,auth=16,sid=38b70ccb,login=1638168992,access=1638168992,saml_lo
gout_url=no,pip=X.X.X.X
[2232:root:3]deconstruct_session_id:694 decode session id ok,
user=[prateek], group=[],authserver=[My-LDAP],portal=[web-
access],host[10.5.27.2],realm=[],csrf_token=[6254EE3AC06AF4B53A89C123D215
C7],idx=0,auth=16,sid=38b70ccb,login=1638168992,access=1638168992,saml_lo
gout_url=no,pip=X.X.X.X
[2232:root:3]req: /remote/fortisslvpn
[2232:root:3]deconstruct_session_id:694 decode session id ok,
user=[prateek], group=[],authserver=[My-LDAP],portal=[web-
access],host[10.5.27.2],realm=[],csrf_token=[6254EE3AC06AF4B53A89C123D215
C7],idx=0,auth=16,sid=38b70ccb,login=1638168992,access=1638168992,saml_lo
gout_url=no,pip=X.X.X.X
[2232:root:3]deconstruct_session_id:694 decode session id ok,
user=[prateek], group=[],authserver=[My-LDAP],portal=[web-
access],host[10.5.27.2],realm=[],csrf_token=[6254EE3AC06AF4B53A89C123D215
C7],idx=0,auth=16,sid=38b70ccb,login=1638168992,access=1638168992,saml_lo
gout_url=no,pip=X.X.X.X
[2232:root:3]req: /FortiClientSslvpnClearCacheUrl/for/Wini
[2232:root:3]def: (nil)
/FortiClientSslvpnClearCacheUrl/for/WininetLibrary/1/2/3/4/5/6/7/8/9/0/a/
b/c/d/e/f/g/h/i/j/k/l/m/n/o/p/q/r/s/t
```