|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | |
|  | | **Palo Alto Remote Access VPNs using SSL** | | | | |  | |
|  |  | | | | | | |  |
|  | | | |  |  | | | |
|  | | | | Weizhen Chen |  | | | |
|  | | | | —CCNP—Jeffery Mason &Michael Hansen |  | | | |
|  | | |  | | |  | | |

Purpose

The purpose of the lab was to learn how to set up a remote access VPN using Global Protect on Palo Altos with SSL.

Background information

Palo Alto Networks is an American Multinational cybersecurity company headquartered in Santa Clara, California. It is known to produce cloud-based firewalls that are highly used in the IT industry. With features such as identifying, controlling, and inspecting encrypted SSL traffic and applications. Including real time low latency content scanning to protect users from viruses, spyware, data leakage, and application vulnerability powered by a stream-based threat prevention engine. And its performance does not downgrade as more security features are enabled. Global Protect is a VPN that provides a secure remote access connection for users to connect to from any place. It assesses the device’s health, security posture, controls and inspects traffic from any device before allowing users to connect with the Global Protect client through a web browser and accessing any sensitive data. A remote access VPN is a Virtual Private Network that allows users who work remotely to securely access and use apps and data that are in a corporate datacenter and headquarters. It makes the user seem like it is in the location of their workplace environment as it encrypts the traffic between the user and the server to have a secure connection, so the user won’t have to worry about the data being intercepted or tampered with. A clientless VPN would create a secure connection between the user and server in a web browser without the need of a client on the device, this gives any users an advantage of still being able to access any apps in the case where the user cannot install a client onto their device. Certificates or secure sockets layer (SSL) certificates are files that are hosted within the webpage that would hold the data that browsers access when you use that webpage. The SSL certificate has the website’s public key with information specific to the site’s identity. For SSL encryption to work, you would need the site’s public key, that takes place when your browser connects with a site with SSL certificates.

Lab commands/Configurations

**PA-410 Configuration:**

config {

mgt-config {

users {

admin {

phash $5$eftfahiv$lEx2H1biYTXVvPnkHwCice.wV8MEFpjts0J2y2f/HU8;

permissions {

role-based {

superuser yes;

}

}

}

}

password-complexity {

enabled yes;

minimum-length 8;

}

}

shared {

application;

application-group;

service;

service-group;

botnet {

configuration {

http {

dynamic-dns {

enabled yes;

threshold 5;

}

malware-sites {

enabled yes;

threshold 5;

}

recent-domains {

enabled yes;

threshold 5;

}

ip-domains {

enabled yes;

threshold 10;

}

executables-from-unknown-sites {

enabled yes;

threshold 5;

}

}

other-applications {

irc yes;

}

unknown-applications {

unknown-tcp {

destinations-per-hour 10;

sessions-per-hour 10;

session-length {

maximum-bytes 100;

minimum-bytes 50;

}

}

unknown-udp {

destinations-per-hour 10;

sessions-per-hour 10;

session-length {

maximum-bytes 100;

minimum-bytes 50;

}

}

}

}

report {

topn 100;

scheduled yes;

}

}

certificate {

RootCA {

subject-hash 7e259cf5;

issuer-hash 7e259cf5;

not-valid-before "May 4 20:06:03 2023 GMT";

issuer RootCA;

not-valid-after "May 3 20:06:03 2024 GMT";

common-name RootCA;

expiry-epoch 1714766763;

ca yes;

subject RootCA;

public-key "-----BEGIN CERTIFICATE-----

MIIEzTCCArWgAwIBAgIUBGrrqf97HdEYix2TOSPh1yhl52MwDQYJKoZIhvcNAQEN

BQAwETEPMA0GA1UEAwwGUm9vdENBMB4XDTIzMDUwNDIwMDYwM1oXDTI0MDUwMzIw

MDYwM1owETEPMA0GA1UEAwwGUm9vdENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A

MIICCgKCAgEApUpC9aEnUbAzjXhqX2RPQAPse7GhdnbVyyX9zQ1IjQ0RFr9goK2g

O+vJDap/uLvoTtytygR6u5RCyKdBzmaFalfwaVtv+qoTBkMICVRjBrExKccEcnTM

UbHqXlDbegToFpQeJ75ZSF5Km3G/AUmpt66q0N4ocHysVYuFsmUS4Bz1M+Tvar6H

OTUO3Db1EWBt7VkZTyEsfnC70Y4MxmNZbR9yjHe56BcVS1lYyvjA6zpj0tnYT/+H

JvGone5/TGL7e0nBs4tD3VnS+bCGkht86gc/+LC/V3LTQfg6PEv/NLMHI+clmWie

7u5gZynw1YKn6ceqNLB54BTFHWCgDOahncipLuNin7ehR1jQe+5BReb6h9JdBCk9

bWMpYfg2irrOFmqkRjxPhgFEtHeQ2E5gVwl13W77hGBjb8vlKgnVgMbY4BurWje9

hxHRRs4AZ/938mMNIVbWfRv1s2borJeP1tpX8od2oT5M5T7sNnGc+JxQe8chtwJM

F/BXuj4pxsiWjGFhh+DHtnQU3yzuK4TiOksDhYhqZl5fqHojD4RslfBpPY+clu6N

/XOpDmlWA/d5ZhB9nKg5h1k6zI2famYLh9VvCxBfZNL3G7lSwjDRZGSUkqQu9qlO

LaQsrfsM7lvgmAsDvz6A6Mr7LQitK1E747zFOwquKM2xldyk4fwfKKMCAwEAAaMd

MBswDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCAgQwDQYJKoZIhvcNAQENBQADggIB

AH4aucQ4oDfp/JMlE1IhmDvh/Of1golsdF0vJLTBmMhjl13MQVymS8+FgnPW5xyv

fnPjL2DAcewk1sc+UhiKWpmA2MWQQ1c9gKBQkd0BPwWEOUynRfOpYdjKhXhzaE/3

UOxO/FQtKeMzsEfvX5/a+ckGJloEHvMYprA+d2T6T9zefbhOM3878UIE9K+Z9QSK

h61UNrsTPGlN29jcpNGPOiviANW2po48yPjV10OGFrY13nK9r76eMJrMU4uJt70Y

A8PzaAYaNc9v+G84u6y/OS6weeD/m9jPkb+btFrsUYWqDjoDwnzpB2tAuoI1LS3n

Fj7KT4xs41IWahFXcebMe5wnUqLGz63TmSrsHm4XsBlZRCYs2575O5ccd31xVq7T

8fvBc3Z0u9o+B0zE+QG59AYPktVGFj89Xc51nUFO+onzsf0qZP9QWKmtub8k8KtG

O/X/ecsBcS4xndSnrx7RbjxUaR/jvg9oPgAIh82oPiUYE/z3mSvz2SYS9Wz/5k1f

HRzZtqAGT/Wk8N3QqRu5VAbhA2Fff9CrhxvlETp18jWGya083gbYUf9AhITp35LB

KZ7ScEGUGukybKw5chtC7O7YlHOQX6dV2L+dlznup33WmFDYZfOvaHq7InRMGnms

lx1jZmifqK9nc71fyEV1ZNnzrjw7d0PblY2mNbwjQ2IH

-----END CERTIFICATE-----

";

algorithm RSA;

private-key -AQ==nOHBFcF1SW788PtLVkMwzcnkodA=



;

}

GP-VPN-CA {

subject-hash 0f276ae7;

issuer-hash 7e259cf5;

not-valid-before "May 4 20:06:46 2023 GMT";

issuer RootCA;

not-valid-after "May 3 20:06:46 2024 GMT";

common-name GP-VPN-CA;

expiry-epoch 1714766806;

ca yes;

subject GP-VPN-CA;

public-key "-----BEGIN CERTIFICATE-----

MIIEwDCCAqigAwIBAgIEalFNBDANBgkqhkiG9w0BAQ0FADARMQ8wDQYDVQQDDAZS

b290Q0EwHhcNMjMwNTA0MjAwNjQ2WhcNMjQwNTAzMjAwNjQ2WjAUMRIwEAYDVQQD

DAlHUC1WUE4tQ0EwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQD61zjP

uwW94I8/yaVmj7KRNc7D6WcZZOSBFgN2qa89NA3QAiLONVeT6XGwW48j4QSPifcy

93sb51WYJcDV3ZamrX0jBi6/ZRJLDknqRgigaxXsKZ5nB0D9xZDakH5GqOCZZcRo

+RRZy3tsaUv2ON08InJHsirCo2D6Zcn2OKEY9JWmm7njdK/xTeMd3LCEA/K8zjan

n2f6PLeZmdCWRvRLkH+0eQLPTflPPhTsS7q6BJwFek/AWTswPmmGdmRmsaDqzOfe

ajXzJWw5T21ZFrQhB0uXz+AdTHI9wPaSg8iXtE4sPP9N0JcQThWoDMuxZ7pX2AYW

913W7LXtJQkmQqONQFItjK/7n63UDjkg8cqJGT76seczZdN68YFBsax/cB67ae2V

8WxrFKnNd4Wdeh/OWkM7SG7J3tALzRtaHZb1MiQz+3swM75xjbz4AK3gR4xbUkeX

5uCuM2TBOkv4RIx29+Z2cKQgU37/oGZqm8dg9u4c/KbBUA28p8jDD1BzzFJaWsdZ

2U17iNPe8QCoXEQE1G7vJtnnKZ8MniiULH9NgSoNNn5S+zvOdKhru0lodgL1Khup

BwsWEn3L4AwBwwWvktcNqfw1fiMrmGLc1XhcCc5qAUXb60Dz7kVpnR/v3n4lwzRX

kK/zY+s6S+UHRYFR6XTQxYejFurGcVcSWaQ56wIDAQABox0wGzAMBgNVHRMEBTAD

AQH/MAsGA1UdDwQEAwICBDANBgkqhkiG9w0BAQ0FAAOCAgEAUc45EnwXnkG2TlQU

Bq+ePmK3nWNryUkD1rAX1bM6itHTcjN5ZqwPF9Vd6xyVMyO/uWBK8YYSmYmhDdvA

1hrkjTikwNFSY2xSCqVt6cIYg2JGoFGiB8sa9IXTHjNTP7OLvzdY5m6Xx1uTasQE

DQj8QjZFNLPw5vWN2B1axefOxoMMhUVH2AFZL2/0CeKJG0dN14uYaimBJ56N1S89

d2FafEMFfOfKAE48cEQntTRqjheb0g7TKD8iBF/MTmAk2Oe2dHSPJfTcyWSeCqmX

lGLBUcv/P4LEvaeFcXQTbb4rJjtOYDXgcu8H7FbLDsD6yd+Mcc4ShiAOo+OS0MQ0

6mw8K2qm8VphmzxpVkvwIkVfM3lyU32cceflUWORukALZS80rIPxeFSKPD9jp5LN

ALanKfcsUzUHaEvho6PeUuDPNa95eyTF//QiNaB7640ZlQfMbSNRUVl0sg1tC65L

Z6Ts60GtSHdIKo8xCXPND+bDVVW5CSNMWfoQQxDKR7uSQVgx9BjBeXJRpgkgHCeW

XHZrRVFh3B0w6YbQFscLAhr1McaURYgVR2myclpwNYDtzEDBjexKlO5OHHtNyoqO

b84DAaFXEyalciRF8TD/i412u88ZNvtc570FBSUM6we0qYM4ehWfL44qZM16p9Hi

9raqGT3U1/0SrkBb8aJupPN0b1w=

-----END CERTIFICATE-----

";

algorithm RSA;

private-key -AQ==cS06NxP5i03oCpVC1kreWfuHdzQ=



;

}

GP-VPN-Client {

subject-hash 4676f1ed;

issuer-hash 0f276ae7;

not-valid-before "May 11 19:52:22 2023 GMT";

issuer GP-VPN-CA;

not-valid-after "May 10 19:52:22 2024 GMT";

common-name GP-VPN-Client;

expiry-epoch 1715370742;

ca no;

subject GP-VPN-Client;

public-key "-----BEGIN CERTIFICATE-----

MIIFFzCCAv+gAwIBAgIEalFNCzANBgkqhkiG9w0BAQ0FADAUMRIwEAYDVQQDDAlH

UC1WUE4tQ0EwHhcNMjMwNTExMTk1MjIyWhcNMjQwNTEwMTk1MjIyWjAYMRYwFAYD

VQQDDA1HUC1WUE4tQ2xpZW50MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKC

AgEAs7ZvITekE6beWPVe3WnKZl8a2Mu7AA2umxsbmliLI4/hef+tNsiYX27Lj92l

LkW4803btCUSQvLSV35jtOf6/U8Xu4L3VOdJ6EB3cbCJKRRaUiLvT857oHdy4r9+

bMYzS2KtkzP1IUGO3MQ83l6ZlyaViG4JHLI1YekBysIAMaPPoXGis31izsu/ppRm

MZDvbsIlEsbF6WkFGCw4Wemwc4RKoMUbJp0DyAVOZ2VC2NCmhUwUm77RHQQLPlW+

0vqflOU88IS742xE1Sc+Qp9sWXBXDBlThDiusDZVvytEVOvXOpyx0tqZb2E+NNDr

y2tkNjWMzcGO5z9/Nsjkgf2zU4MZgwoUwPtZeN9/Z5JTeHPz2mRoVwweZ7hD7rCB

7DrHPZBh25uA9/9hw2ajavZSIehUiCd+INAPquUdnvYdMUIwo37iZCuKEwiZMI45

rCLLEfges/37QNoUfcideA5KkP1Qeiso6RjoImQD7R4X68uj8SSJNb6WGR7OTF81

xFGeicUMyjsmGO9wF2Gsk6l6e9AqkUxbULXG3gRXsdRbYzK1lFkzCq48MFZ8JbBn

RaWKe02x6qZzcLPYl3xMWxwa/T+YdpKLPxkmW1cE0IR3Cah+g7BZccFgIS8DDt98

Bsfn8XECCfhVptaQws+thmXKsN5nTuEWUYGm0p9EPc7hCf0CAwEAAaNtMGswCQYD

VR0TBAIwADALBgNVHQ8EBAMCA7gwJwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUF

BwMCBggrBgEFBQcDBTAJBgNVHSMEAjAAMB0GA1UdDgQWBBTzP1+nQWSG+4CuNHnR

t/swRQ0l6jANBgkqhkiG9w0BAQ0FAAOCAgEAjto/EMuhn0DHNM9AX7+IL6RfJxdL

JlwQ/xNQXoVOokm8ELsUCi5q/b5arGHcfAFPl/kJc+jIasxhDBq7MBOyZVIMpEPq

xHAaEvm2RuqhKhCYLQ9Qnykn8zRbhGYoNqVMnH20lAx0atIrOezXohmlFuf93bZ3

FqBNX3zRtFuCnc4d5GaKUPBuvXCm4zjG9pGsFSLIcU+/de2EXLqxOH515cBJV+xd

GqYy+qD6MWpGUrcnZPdcG9knQyKL0YFuc9U+yVz9VbRlCeRKb1nR9lhcwKJa6TJM

M5pKz2bCPF3y3us8efeXiXteDoAhtfQ2h4mA4MAKPQqzUUHgUv8LF6ePYwUoIkyv

nYJ6EgTrBlj4yycjDI9be5NMaXa+QzcI6LGKXbxb1RwoLh8SdGA6CtbY37N/tS+Z

v09QTSWnOJJpymMaNYycBaHEPieKZQ7jdXBD5ebPFQ9NmfbRi/M6navy56dwfBXD

sYZRKyaUbTkvHPGAJgq/ksvyuM+pn23loHpopt93Q7HqsOxu0A8dhL/Borx268u4

/yzFsekKA2yh1crqC8CDk+o18VmXAxlAS4OZats55o+W0jIikSPY/0bRlvcdEx0N

G8rxA8RNLWBiQsKKKDvLt9ED9ML2r00rcjyt2UKdurlaQ1V8sD7c1V8TjwzDvc8Z

WLLNg4yzhhUk5Ng=

-----END CERTIFICATE-----

";

algorithm RSA;

private-key -AQ==z/9x9fteid0tE6jcNUUfBK+7ino=



;

}

GP-VPN-Server {

subject-hash 58d5ca8f;

issuer-hash 0f276ae7;

not-valid-before "May 15 14:22:55 2023 GMT";

issuer GP-VPN-CA;

not-valid-after "May 14 14:22:55 2024 GMT";

common-name 192.168.40.218;

expiry-epoch 1715696575;

ca no;

subject 192.168.40.218;

public-key "-----BEGIN CERTIFICATE-----

MIIFGDCCAwCgAwIBAgIEalFNDjANBgkqhkiG9w0BAQ0FADAUMRIwEAYDVQQDDAlH

UC1WUE4tQ0EwHhcNMjMwNTE1MTQyMjU1WhcNMjQwNTE0MTQyMjU1WjAZMRcwFQYD

VQQDDA4xOTIuMTY4LjQwLjIxODCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoC

ggIBAL94l4Jam/p2oSymP5PeATfpmIO5d/lMWcF08XA0gcK2K52cJEs+0zRVgDji

TMcivYuya84ZuPexnnoMtJCr0KxNqf15mcanJ2KnWWYtTnk1IA1POsjss4F3ccvl

VLjI197w4JxquqvPuN/6lFuZrjMFa6oN5xn6BwGeOJfXHW1U8TVNA6zRxoK4JPvf

9U52ue0IXa8SR3SWq2A4hFHFqUN752tDKjifkFCpy758cUY7flgB/ppUIEKV6yoz

Rtow1iHjTRncZGRw1nDtvOsOSB/84zjoccyA2oduYjleGLYLhgpgXW1VTF1Bbb5t

h7ape2Eo3CzUW6k7tvYaOxy+dLuOXBvMp6T+jJoXmoKcsXOM4i48RXXqlzSB7c1a

6dAiB+L4LWeXKulsajqmRzGfu0irZMxY6zlFkkew5Z7w+NC25ZiEI64vNnkCTLCL

XWLZIUEithaF9XQWJ6zvSP/XRvI/JQAvYLnxOHUpa9QeyaAoNIgTyaGV5OVUySx3

gxxI3n1F9jSXyUkqTwYkbvcRIPzif2rZdks9ox5jhDV3ZUQ1MT1UL8nvBPiXZbVS

lhpL089KG1aujuqkLoDZzkKFktKiJG5MAf+2RuOEjnL6An7S8Z5AigWwKIfz2CuT

wG4+Kmay7UvFEos1U5Pkx0ahqWx/gNyCXras6wDoXFtgyOFZAgMBAAGjbTBrMAkG

A1UdEwQCMAAwCwYDVR0PBAQDAgO4MCcGA1UdJQQgMB4GCCsGAQUFBwMBBggrBgEF

BQcDAgYIKwYBBQUHAwUwCQYDVR0jBAIwADAdBgNVHQ4EFgQUv9GJPs3FG+oGDS0X

vXllEapbw6kwDQYJKoZIhvcNAQENBQADggIBAC9q9nJl9h5UQfMLQdLlQAfQpLwP

wk2bRi3f3ZNLNP7R0RHbpalCENIiyoNFh0n0R/NA44j/GkJBb9Zej4+tSAWwXNnA

pOgaSRy6VENGyBjL68/upbNFM9ARvHqL9LCDnAdclcSYZoDrYfhYnEXHVS7iNCws

9rX5oUpeRLymxgnSrX78MVXs2SLrrG/NqvCXwzKfwQLT3t9jsp1EDNkvVgHt4WfE

Sbv1zIHlLneJgqHcxT93pnuDFMDxDXLxFeIINu0XDDL+Y1pfsfwU8QBwq+pFYUzb

+hx7LYsAPw2zIBM5oBC+61OEUzAXeLP52ajq9SbSdk0B5oxBUraHr7LHC1ETkVw7

l2COK7iLGNqaXqPqTaVCgMrd7TAku29p3zKbzSVRmkGZ7y0uJv8cruQfGIG2ZkOk

VnWTuF1NHIXpheebtDEdqwIH8vK9jyvsnRSeFuSMVYBP6vN7JcAg3e+sMRydjXS9

wJ3CfivNfwaBIEVNrG1zaVIXopQBXHOWaVguhOpymFPozpoTsxtHn2O82Zi6Ui9r

MIstz4P+EWadT4hCNf7A5i7mJCe9pLVv8RbCviTLsv2Qm4GupA6QJSVNvfD3v4q2

szICC99R0jvcd/bhiazjo7aTLGA66ecPMXNAd1TlsZANY36BeV/cJILD92hQToqn

xQoFril7Lzzt63rP

-----END CERTIFICATE-----

";

algorithm RSA;

private-key -AQ==xDj6igW1VpQt5id/LmHXJ/7UOqQ=wfL5Zc+wUAak+B7CnAVY6NdutYWtt67XvF+yGHFGS+v7ACsCjMFMk7rZ8Z7/nntTCBTAw3DjIw7sLXQxx7ZkPBE2iuNoeL3FTXIV+yjgLM38ArSUSO4acIdQyfLNg1ccVeWXmrh2HmAg6aU95qR6N3r9JS1Fes4o0qU1CFhyBUHSEF1TPQqvosiEhc19/3UjrQAn9iLaqF0T/pKemnpwz065hsPSNoH3dC6loklc4B2mL3KXmNYbKTaLIb4h8tS/w9bvzeHEjNIL7UPdrcLQ4c92fvo4OheoxK76Z1su48awMnB9uMltCmRu+DOSEO06Q7bF/91VuHzwpZZPCPNbchlVbqrPEwkfyyfoagXSo2nkgiphEooVdIqp/xlQHhqlBQbdQlHzuyckgz7rTDqTx6l3LJPzdNqCVyOQJlibIVWNHke01Qp3OP4dPKPafXYL





2oA6k7zphXGoam37JUqSwUUqVRmr4E4udgCwe6NXAjt3+EhS5tHqSZcG1eDO6O8rsgBaV5yk/a55Rwteas3+/BdBu8ydget1/ZRFHT7MK6kESu44nMqV3cwa7EO5rDNCQH/2T/207NNR0l5w=;

}

}

ssl-tls-service-profile {

"Global Protect" {

protocol-settings {

min-version tls1-2;

max-version max;

}

certificate GP-VPN-Server;

}

}

authentication-profile {

"Local Database" {

method {

local-database;

}

multi-factor-auth {

mfa-enable no;

}

allow-list all;

}

}

local-user-database {

user {

remote {

phash $5$vtjvxgtx$3mW0GN/7GY2MX9RHEB5LfTjvRDbUzsQwklWRgajKCN2;

}

}

}

certificate-profile {

GlobalProtect {

username-field {

subject common-name;

}

CA {

RootCA;

}

}

}

}

devices {

localhost.localdomain {

network {

interface {

ethernet {

ethernet1/1 {

layer3 {

ndp-proxy {

enabled no;

}

sdwan-link-settings {

upstream-nat {

enable no;

static-ip;

}

enable no;

}

lldp {

enable no;

}

dhcp-client {

send-hostname {

enable no;

hostname system-hostname;

}

}

interface-management-profile Management;

}

}

ethernet1/2 {

layer2 {

lldp {

enable no;

}

}

}

ethernet1/3 {

layer2 {

lldp {

enable no;

}

}

}

ethernet1/4 {

layer2 {

lldp {

enable no;

}

}

}

ethernet1/5 {

layer2 {

lldp {

enable no;

}

}

}

ethernet1/6 {

layer2 {

lldp {

enable no;

}

}

}

ethernet1/7 {

layer2 {

lldp {

enable no;

}

}

}

}

loopback {

units;

}

vlan {

units {

vlan.666 {

ndp-proxy {

enabled no;

}

ddns-config {

ddns-hostname system-hostname;

ddns-vendor paloalto-networks-ddns;

ddns-vendor-config {

ztp-ddns-ttl {

value 30;

}

}

}

adjust-tcp-mss {

enable no;

}

ip {

192.168.20.1/24;

}

}

}

ipv6 {

neighbor-discovery {

router-advertisement {

enable no;

}

}

}

ndp-proxy {

enabled no;

}

ddns-config {

ddns-hostname system-hostname;

ddns-vendor paloalto-networks-ddns;

ddns-vendor-config {

ztp-ddns-ttl {

value 30;

}

}

ddns-enabled yes;

}

adjust-tcp-mss {

enable no;

}

}

tunnel {

units {

tunnel.666 {

ip {

10.10.10.1/24;

}

}

}

}

}

vlan {

Vlalto {

virtual-interface {

interface vlan.666;

}

interface [ ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5 ethernet1/6 ethernet1/7];

}

}

virtual-wire;

profiles {

monitor-profile {

default {

interval 3;

threshold 5;

action wait-recover;

}

}

interface-management-profile {

Management {

http no;

https yes;

ssh yes;

ping yes;

}

}

}

ike {

crypto-profiles {

ike-crypto-profiles {

default {

encryption [ aes-128-cbc 3des];

hash sha1;

dh-group group2;

lifetime {

hours 8;

}

}

Suite-B-GCM-128 {

encryption aes-128-cbc;

hash sha256;

dh-group group19;

lifetime {

hours 8;

}

}

Suite-B-GCM-256 {

encryption aes-256-cbc;

hash sha384;

dh-group group20;

lifetime {

hours 8;

}

}

}

ipsec-crypto-profiles {

default {

esp {

encryption [ aes-128-cbc 3des];

authentication sha1;

}

dh-group group2;

lifetime {

hours 1;

}

}

Suite-B-GCM-128 {

esp {

encryption aes-128-gcm;

authentication none;

}

dh-group group19;

lifetime {

hours 1;

}

}

Suite-B-GCM-256 {

esp {

encryption aes-256-gcm;

authentication none;

}

dh-group group20;

lifetime {

hours 1;

}

}

}

global-protect-app-crypto-profiles {

default {

encryption aes-128-cbc;

authentication sha1;

}

}

}

}

qos {

profile {

default {

class-bandwidth-type {

mbps {

class {

class1 {

priority real-time;

}

class2 {

priority high;

}

class3 {

priority high;

}

class4 {

priority medium;

}

class5 {

priority medium;

}

class6 {

priority low;

}

class7 {

priority low;

}

class8 {

priority low;

}

}

}

}

}

}

}

virtual-router {

default {

protocol {

bgp {

enable no;

dampening-profile {

default {

cutoff 1.25;

reuse 0.5;

max-hold-time 900;

decay-half-life-reachable 300;

decay-half-life-unreachable 900;

enable yes;

}

}

}

}

}

RouterAlto {

ecmp {

algorithm {

ip-modulo;

}

}

protocol {

bgp {

enable no;

routing-options {

graceful-restart {

enable yes;

}

}

}

rip {

enable no;

}

ospf {

enable no;

}

ospfv3 {

enable no;

}

}

interface [ ethernet1/1 tunnel.666 vlan.666];

routing-table {

ip {

static-route {

"Default Route" {

nexthop {

ip-address 192.168.40.1;

}

bfd {

profile None;

}

interface ethernet1/1;

metric 10;

destination 0.0.0.0/0;

route-table {

unicast;

}

}

}

}

}

}

}

dhcp {

interface {

vlan.666 {

server {

ip-pool 192.168.20.2-192.168.20.254;

reserved {

192.168.20.10;

}

mode enabled;

option {

dns {

primary inherited;

secondary inherited;

}

wins {

primary inherited;

secondary inherited;

}

nis {

primary inherited;

secondary inherited;

}

ntp {

primary inherited;

secondary inherited;

}

inheritance {

source ethernet1/1;

}

lease {

timeout 120;

}

pop3-server inherited;

smtp-server inherited;

gateway 192.168.20.1;

subnet-mask 255.255.255.0;

}

}

}

}

}

tunnel {

global-protect-gateway {

GP-GW-N {

client {

exclude-video-traffic {

applications;

enabled no;

}

inheritance;

dns-server;

wins-server;

dns-suffix-inherited no;

}

ipsec {

third-party-client {

enable no;

}

}

local-address {

interface ethernet1/1;

ip-address-family ipv4;

ip;

}

ip-pool;

tunnel-interface tunnel.666;

}

}

}

dns-proxy {

"Global Protect" {

default {

inheritance {

source ethernet1/1;

}

primary inherited;

}

cache {

max-ttl {

enabled no;

}

enabled yes;

}

tcp-queries {

enabled no;

}

}

}

}

deviceconfig {

system {

ip-address 192.168.20.10;

netmask 255.255.255.0;

update-server updates.paloaltonetworks.com;

update-schedule {

threats {

recurring {

daily {

at 08:00;

action download-and-install;

}

}

}

global-protect-clientless-vpn {

recurring {

daily {

at 08:00;

action download-and-install;

}

}

}

global-protect-datafile {

recurring {

daily {

at 10:00;

action download-and-install;

}

}

}

}

timezone US/Pacific;

service {

disable-telnet yes;

disable-http yes;

}

hostname PaloLabo;

device-telemetry {

device-health-performance yes;

product-usage yes;

threat-prevention yes;

region Americas;

}

type {

static;

}

default-gateway 192.168.20.1;

dns-setting {

servers {

primary 1.1.1.1;

secondary 8.8.8.8;

}

}

}

setting {

config {

rematch yes;

}

management {

hostname-type-in-syslog FQDN;

}

}

}

vsys {

vsys1 {

application;

application-group;

zone {

trust {

network {

virtual-wire;

}

}

untrust {

network {

virtual-wire;

}

}

Trust-L3 {

network {

layer3 vlan.666;

}

}

Untrust-L3 {

network {

layer3 ethernet1/1;

}

}

Trust-L2 {

network {

layer2 [ ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5 ethernet1/6 ethernet1/7];

}

}

GlobalProtect {

network {

layer3 tunnel.666;

}

enable-user-identification yes;

}

}

service;

service-group;

schedule;

rulebase {

security {

rules {

rule1 f3eb233f-9d71-4e39-9c65-7c85f24ca341 {

from trust;

to untrust;

source any;

destination any;

service any;

application any;

action allow;

log-end yes;

}

"Internet Outgoing" 33c15791-e0cd-4461-97f2-4d421a5c2af5 {

to Untrust-L3;

from Trust-L3;

source any;

destination any;

source-user any;

category any;

application any;

service application-default;

source-hip any;

destination-hip any;

action allow;

description "Traffic going out to the internet";

}

"Global Protect" 506d5f55-ec1b-4d3e-9c85-3778557dcdf2 {

to Untrust-L3;

from [ GlobalProtect Trust-L3];

source any;

destination any;

source-user any;

category any;

application [ panos-global-protect ssl web-browsing];

service application-default;

source-hip any;

destination-hip any;

action allow;

}

}

}

nat {

rules {

"Internet Outgoing" 6392f35b-33e9-491a-956d-98a3a4c37461 {

source-translation {

dynamic-ip-and-port {

interface-address {

interface ethernet1/1;

}

}

}

to Untrust-L3;

from Trust-L3;

source any;

destination any;

service any;

to-interface ethernet1/1;

}

"Global Protect" ca5ec87d-9ff6-485b-9824-9f8779c1ab5c {

source-translation {

dynamic-ip-and-port {

interface-address {

interface ethernet1/1;

}

}

}

to Untrust-L3;

from [ GlobalProtect Trust-L3];

source any;

destination any;

service any;

to-interface ethernet1/1;

}

}

}

}

profile-group {

Internet {

virus default;

spyware strict;

vulnerability strict;

url-filtering default;

}

}

import {

network {

interface [ ethernet1/1 ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5 ethernet1/6 ethernet1/7 vlan vlan.666 tunnel.666];

}

}

global-protect {

global-protect-portal {

GP-Portal {

portal-config {

client-auth {

"Local Auth" {

user-credential-or-client-cert-required yes;

os Any;

authentication-profile "Local Database";

authentication-message "Enter login credentials";

auto-retrieve-passcode no;

username-label Username;

password-label Password;

}

}

local-address {

interface ethernet1/1;

ip;

}

custom-login-page factory-default;

custom-home-page factory-default;

ssl-tls-service-profile "Global Protect";

custom-help-page factory-default;

}

client-config {

configs {

GP-Client {

hip-collection {

max-wait-time 20;

collect-hip-data yes;

}

gateways {

external {

list {

Ext-GW {

ip {

ipv4 192.168.40.218;

}

priority-rule {

Any {

priority 1;

}

}

manual no;

}

}

cutoff-time 5;

}

}

authentication-override {

accept-cookie {

cookie-lifetime {

lifetime-in-hours 24;

}

}

cookie-encrypt-decrypt-cert RootCA;

generate-cookie yes;

}

agent-ui {

welcome-page {

page factory-default;

}

max-agent-user-overrides 0;

agent-user-override-timeout 0;

}

source-user any;

os any;

gp-app-config {

config {

connect-method {

value on-demand;

}

refresh-config-interval {

value 24;

}

agent-user-override {

value allowed;

}

uninstall {

value allowed;

}

client-upgrade {

value prompt;

}

enable-signout {

value yes;

}

use-sso {

value yes;

}

use-sso-pin {

value no;

}

use-sso-macos {

value no;

}

logout-remove-sso {

value yes;

}

krb-auth-fail-fallback {

value yes;

}

default-browser {

value no;

}

retry-tunnel {

value 30;

}

retry-timeout {

value 5;

}

traffic-enforcement {

value no;

}

enforce-globalprotect {

value no;

}

captive-portal-exception-timeout {

value 0;

}

traffic-blocking-notification-delay {

value 15;

}

display-traffic-blocking-notification-msg {

value yes;

}

traffic-blocking-notification-msg {

value "<div style="font-family:'Helvetica Neue';"><h1 style="color:red;text-align:center; margin: 0; font-size: 30px;">Notice</h1><p style="margin: 0;font-size: 15px; line-height: 1.2em;">To access the network, you must first connect to GlobalProtect.</p></div>";

}

allow-traffic-blocking-notification-dismissal {

value yes;

}

display-captive-portal-detection-msg {

value no;

}

captive-portal-detection-msg {

value "<div style="font-family:'Helvetica Neue';"><h1 style="color:red;text-align:center; margin: 0; font-size: 30px;">Captive Portal Detected</h1><p style="margin: 0; font-size: 15px; line-height: 1.2em;">GlobalProtect has temporarily permitted network access for you to connect to the Internet. Follow instructions from your internet provider.</p><p style="margin: 0; font-size: 15px; line-height: 1.2em;">If you let the connection time out, open GlobalProtect and click Connect to try again.</p></div>";

}

captive-portal-notification-delay {

value 5;

}

certificate-store-lookup {

value user-and-machine;

}

scep-certificate-renewal-period {

value 7;

}

retain-connection-smartcard-removal {

value yes;

}

enable-advanced-view {

value yes;

}

enable-do-not-display-this-welcome-page-again {

value yes;

}

user-accept-terms-before-creating-tunnel {

value no;

}

rediscover-network {

value yes;

}

resubmit-host-info {

value yes;

}

can-change-portal {

value yes;

}

can-continue-if-portal-cert-invalid {

value no;

}

show-agent-icon {

value yes;

}

user-switch-tunnel-rename-timeout {

value 0;

}

pre-logon-tunnel-rename-timeout {

value -1;

}

preserve-tunnel-upon-user-logoff-timeout {

value 0;

}

ipsec-failover-ssl {

value 0;

}

display-tunnel-fallback-notification {

value yes;

}

ssl-only-selection {

value 0;

}

tunnel-mtu {

value 1400;

}

max-internal-gateway-connection-attempts {

value 0;

}

adv-internal-host-detection {

value no;

}

portal-timeout {

value 5;

}

connect-timeout {

value 5;

}

receive-timeout {

value 30;

}

split-tunnel-option {

value network-traffic;

}

advanced-st-public-key {

value Empty;

}

enforce-dns {

value yes;

}

append-local-search-domain {

value no;

}

flush-dns {

value no;

}

agent-proxy-port {

value 9999;

}

agent-proxy-mode {

value 1;

}

proxy-multiple-autodetect {

value no;

}

use-proxy {

value yes;

}

enable-hip-remediation {

value 0;

}

wsc-autodetect {

value yes;

}

mfa-enabled {

value no;

}

mfa-listening-port {

value 4501;

}

mfa-notification-msg {

value "You have attempted to access a protected resource that requires additional authentication. Proceed to authenticate at";

}

mfa-prompt-suppress-time {

value 0;

}

ipv6-preferred {

value yes;

}

log-gateway {

value no;

}

cdl-log {

value no;

}

dem-notification {

value yes;

}

dem-agent {

value not-install;

}

quarantine-add-message {

value "Your security policy has restricted access to the network from this device. If the issue persists, contact your administrator.";

}

quarantine-remove-message {

value "Your security policy has restored access to the network from this device. If you still cannot access the network, contact youlines 1

r administrator.";

}

init-panel {

value no;

}

user-input-on-top {

value no;

}

}

}

save-user-credentials 1;

portal-2fa no;

manual-only-gateway-2fa no;

internal-gateway-2fa no;

auto-discovery-external-gateway-2fa no;

mdm-enrollment-port 443;

}

}

root-ca {

RootCA {

install-in-cert-store yes;

}

}

agent-user-override-key -AQ==i+wEBkl8z4u5OTMAW1BNhXhd/BQ=+Yw46SiFiFHyDHlZf4gmBg==;

}

satellite-config {

client-certificate {

local;

}

}

clientless-vpn {

crypto-settings {

ssl-protocol {

min-version tls1-2;

enc-algo-3des no;

}

}

login-lifetime {

hours 3;

}

inactivity-logout {

minutes 30;

}

apps-to-user-mapping {

"Clientless Apps" {

source-user any;

applications [ Linux Entertainment "Search Engines" "Social Media" Software Tools];

enable-custom-app-URL-address-bar no;

}

}

hostname 192.168.40.218;

security-zone GlobalProtect;

dns-proxy "Global Protect";

}

}

}

global-protect-gateway {

GP-GW {

roles {

default {

login-lifetime {

days 30;

}

inactivity-logout 180;

lifetime-notify-prior 30;

lifetime-notify-message "Your GlobalProtect session will expire in 30 minutes. Please save your work before your session expires.";

inactivity-notify-prior 30;

inactivity-notify-message "Your GlobalProtect session will time out in 30 minutes. Please save your work before your session times out.";

admin-logout-notify no;

admin-logout-notify-message "Your administrator has logged you out.";

}

}

client-auth {

GP-Gateway-auth {

os Any;

authentication-profile "Local Database";

authentication-message "Enter login credentials";

user-credential-or-client-cert-required yes;

auto-retrieve-passcode no;

username-label Username;

password-label Password;

}

}

remote-user-tunnel-configs {

Client {

authentication-override {

accept-cookie {

cookie-lifetime {

lifetime-in-hours 24;

}

}

cookie-encrypt-decrypt-cert RootCA;

generate-cookie yes;

}

split-tunneling {

access-route [ 182.168.40.0/23 192.168.20.0/24];

}

source-user any;

ip-pool 10.10.10.2-10.10.10.254;

os any;

retrieve-framed-ip-address no;

no-direct-access-to-local-network no;

}

}

local-address {

interface ethernet1/1;

ip-address-family ipv4;

}

ssl-tls-service-profile "Global Protect";

tunnel-mode yes;

remote-user-tunnel tunnel.666;

}

}

clientless-app {

YouTube {

application-home-url www.youtube.com;

}

Google {

application-home-url www.google.com;

}

RedHat {

application-home-url www.redhat.com;

}

Debian {

application-home-url debian.org;

}

Kali {

application-home-url kali.org;

}

Fedora {

application-home-url fedoraproject.org;

}

StartPage {

application-home-url startpage.com;

}

"Arch Linux" {

application-home-url archlinux.org;

}

Spotify {

application-home-url www.spotify.com;

}

VirtualBox {

application-home-url www.virtualbox.org;

}

VMWare {

application-home-url www.vmware.com;

}

Microsoft {

application-home-url www.microsoft.com;

}

"Brave Search" {

application-home-url search.brave.com;

}

Bing {

application-home-url www.bing.com;

}

DuckDuckGo {

application-home-url duckduckgo.com;

}

ChatGPT {

application-home-url chat.openai.com;

}

Instagram {

application-home-url www.instagram.com;

}

}

clientless-app-group {

"Search Engines" {

members [ Bing "Brave Search" DuckDuckGo Google StartPage];

}

Linux {

members [ "Arch Linux" Debian Fedora Kali RedHat];

}

Entertainment {

members [ YouTube Spotify];

}

Software {

members [ VirtualBox VMWare Microsoft];

}

Tools {

members ChatGPT;

}

"Social Media" {

members Instagram;

}

}

}

}

}

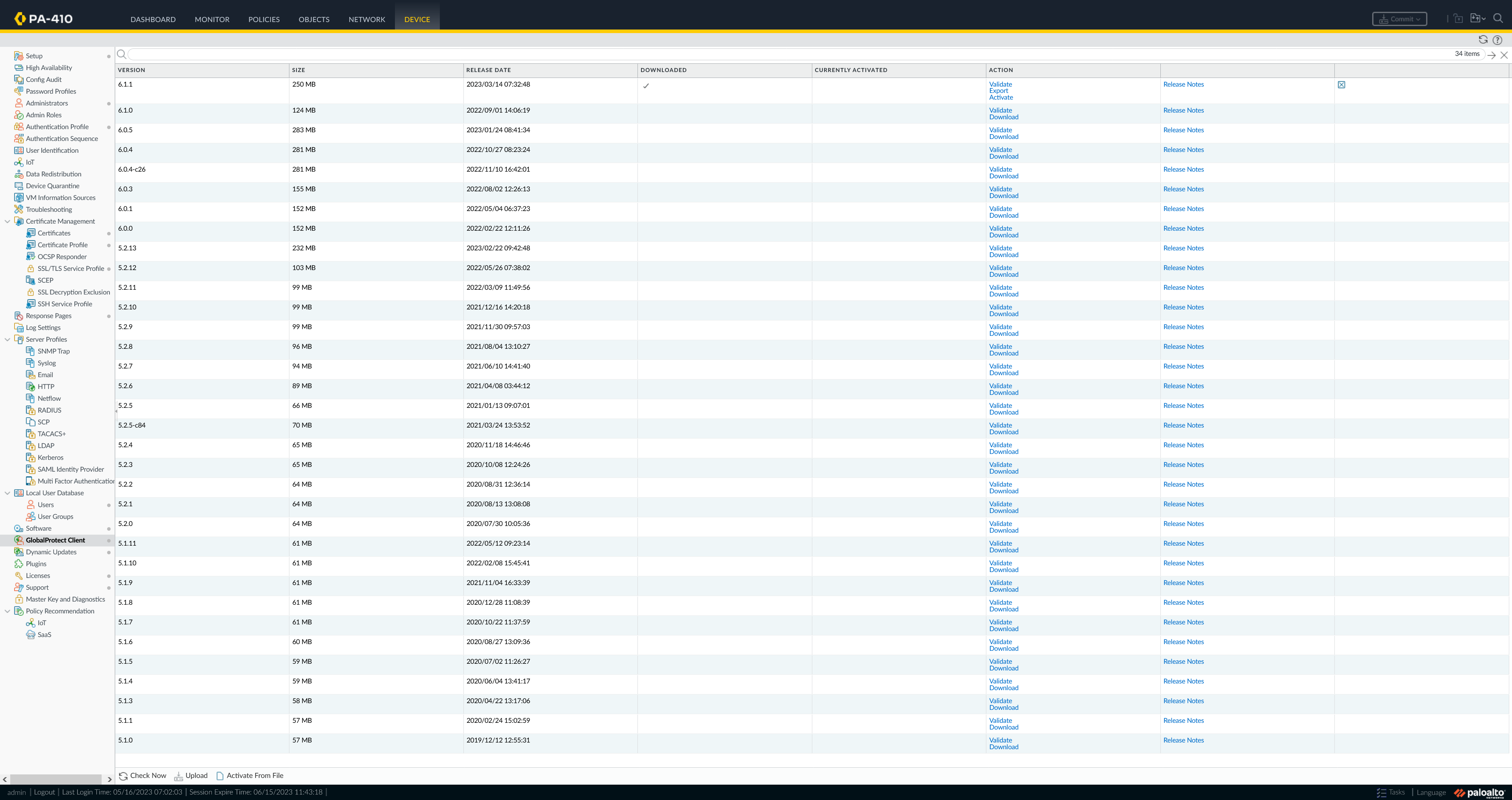
}

}

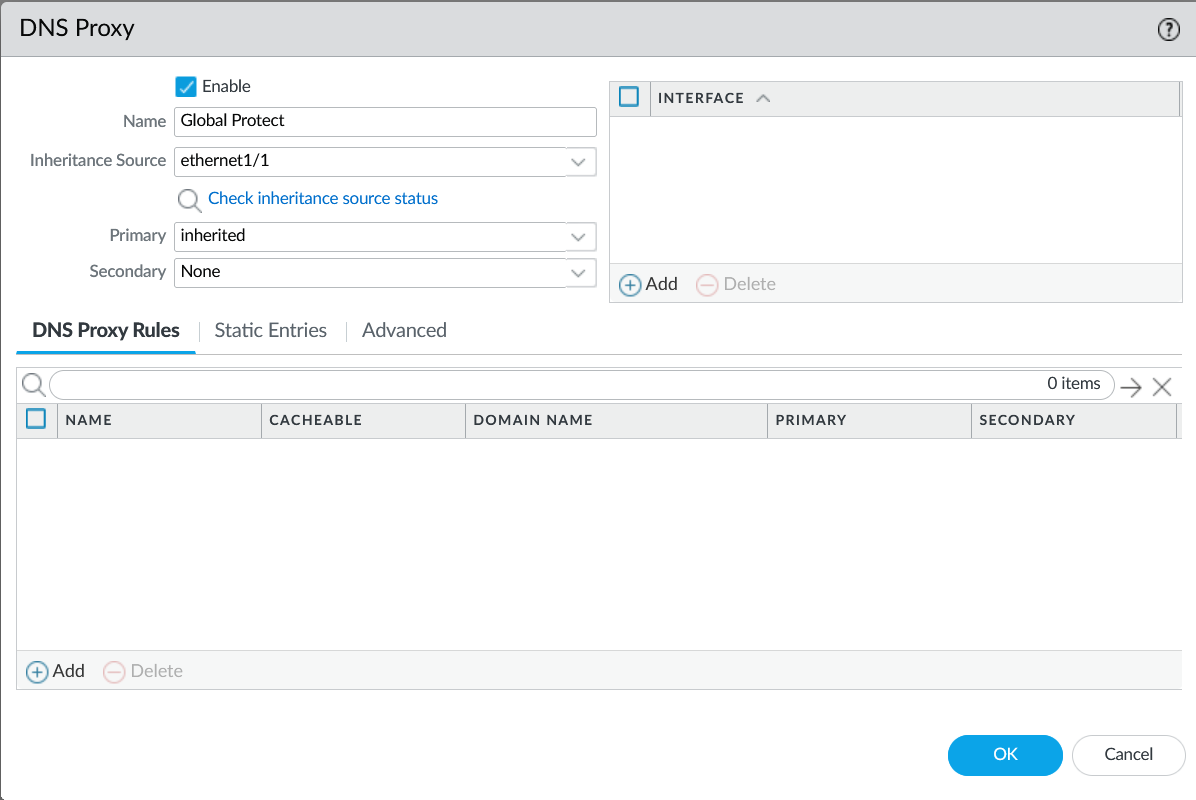
}

Screenshots

Activating Palo Alto Client.



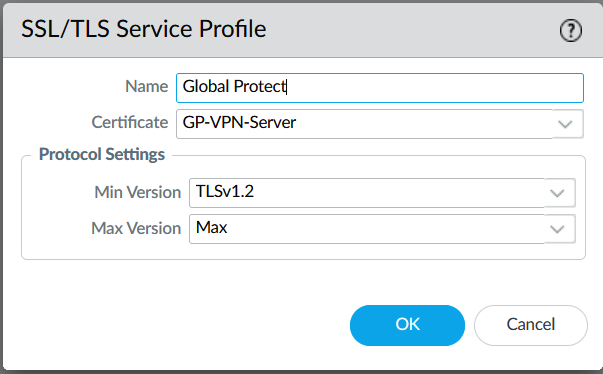
Created DNS Proxy profile for clientless apps.



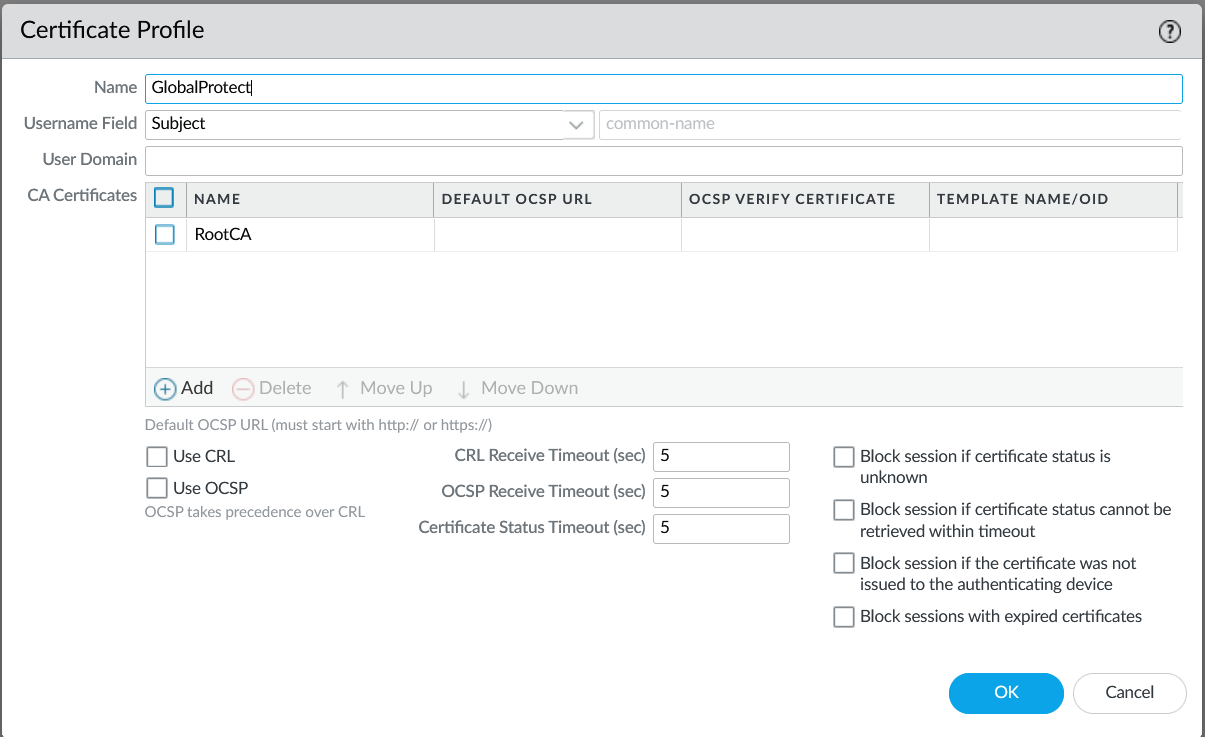
Generated Root CA, Intermediate CA, and Server certificate. The client certificate is for certificate authentication.



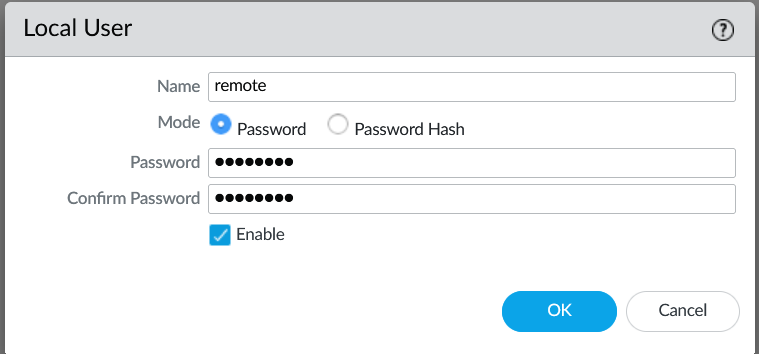
SSL/TLS Profile for the Global Protect portal.



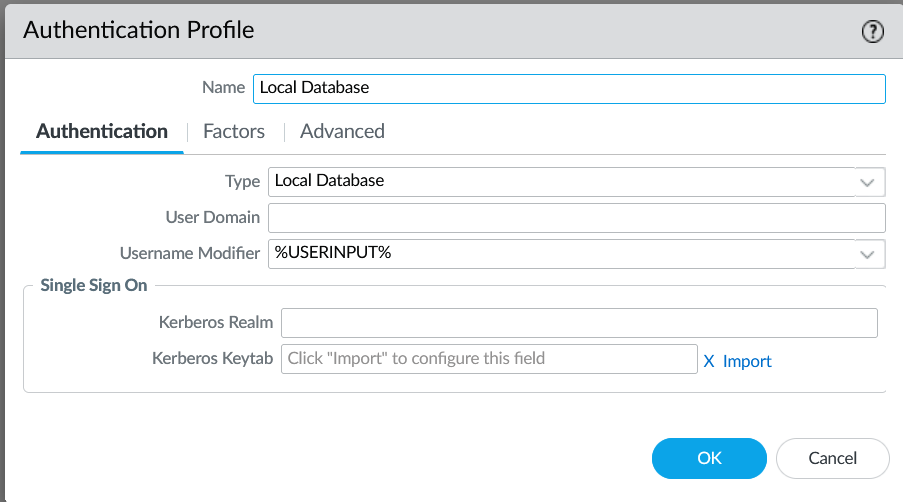
Certificate Profile for Certificate authentication.



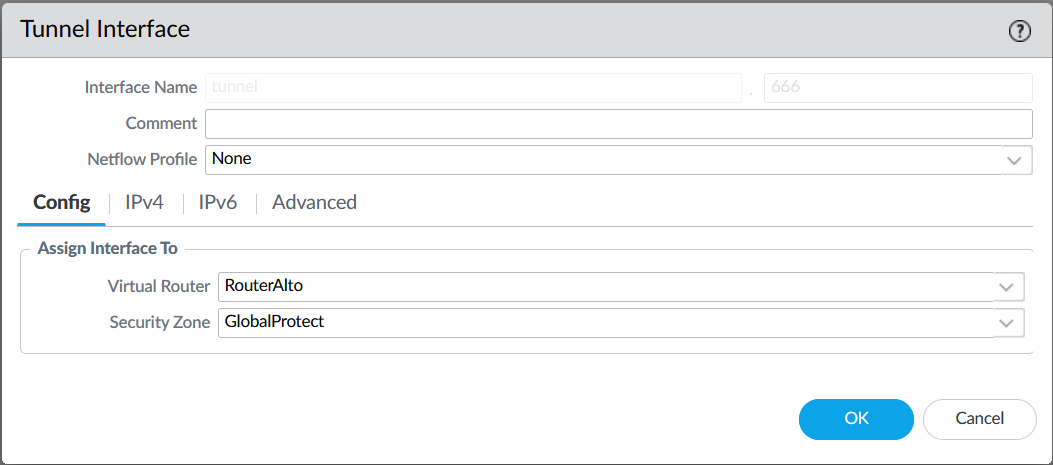
Created a local user that is used for local user authentication.



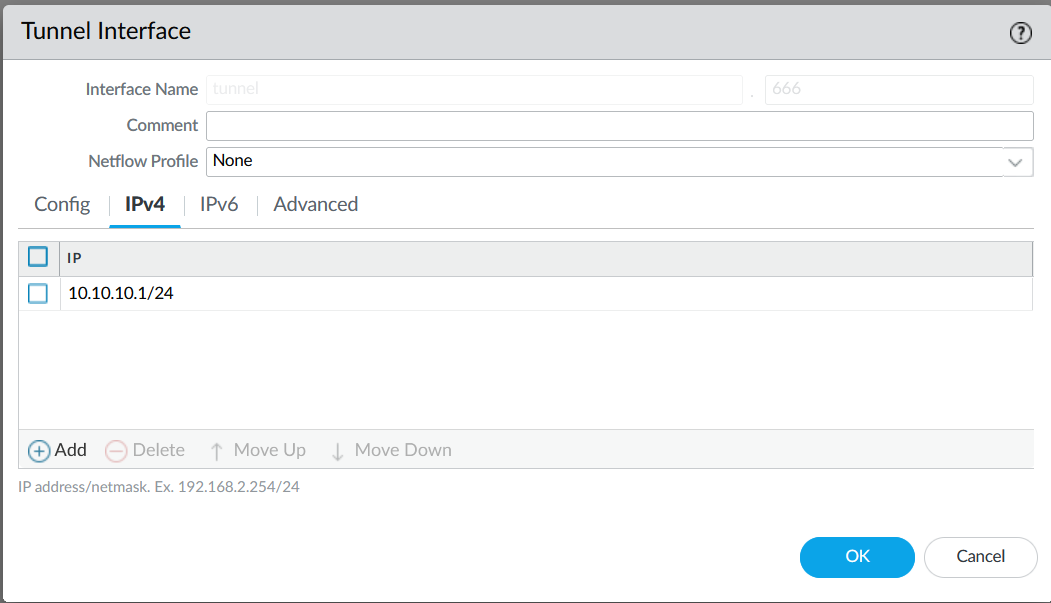
Authentication profile for Global protect to authenticate local users.



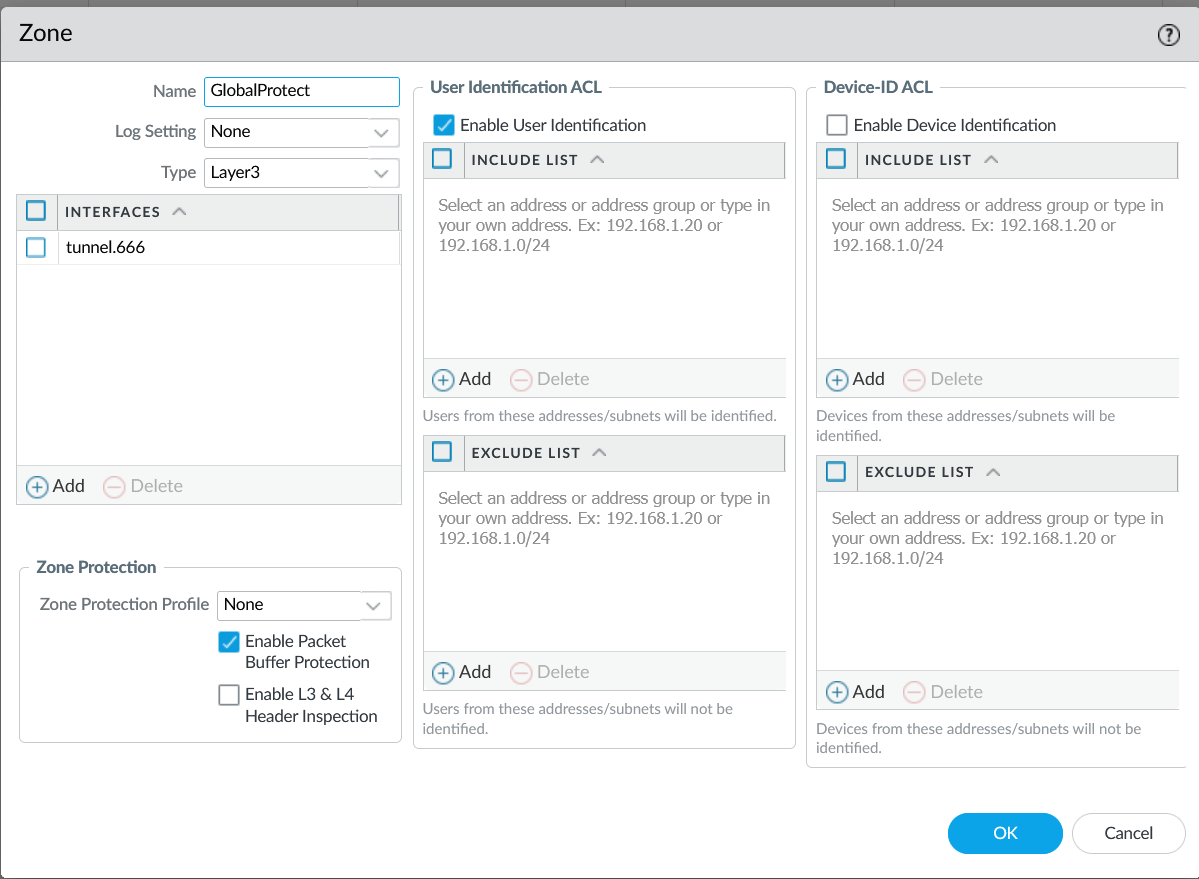
Tunnel interface for the Global Protect portal.



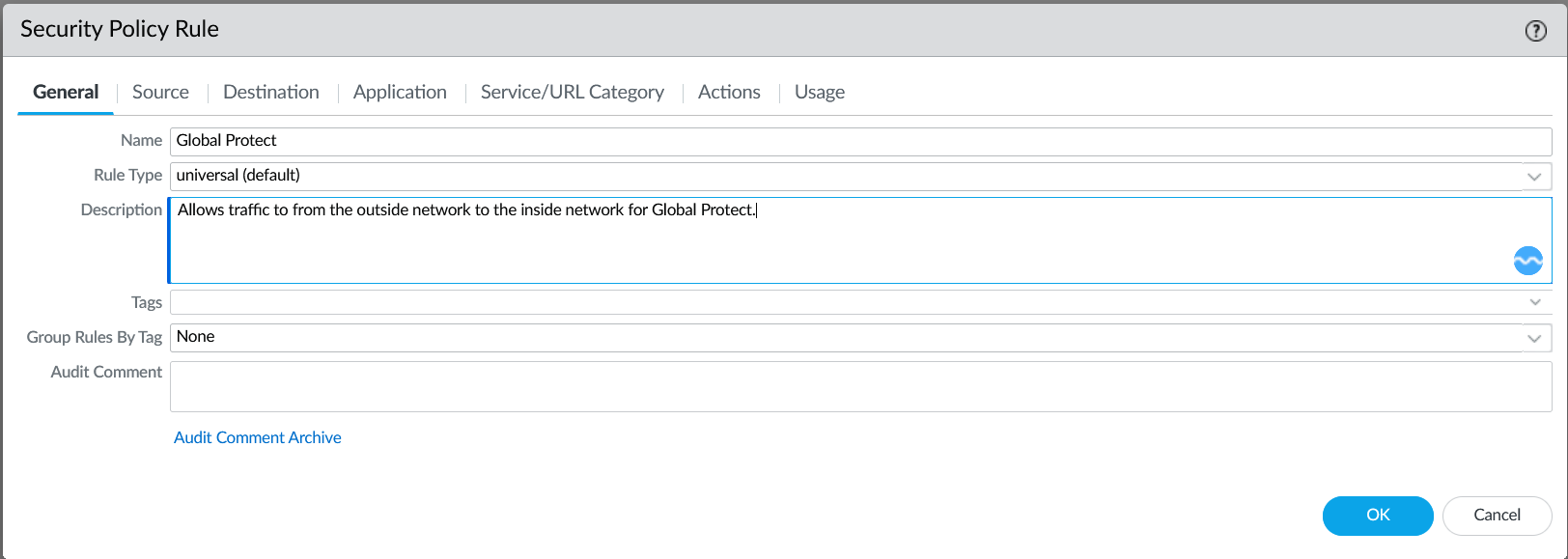
Configured an IPv4 address for the tunnel interface, even though it’s not required it still works with an IP address assigned to the tunnel interface.



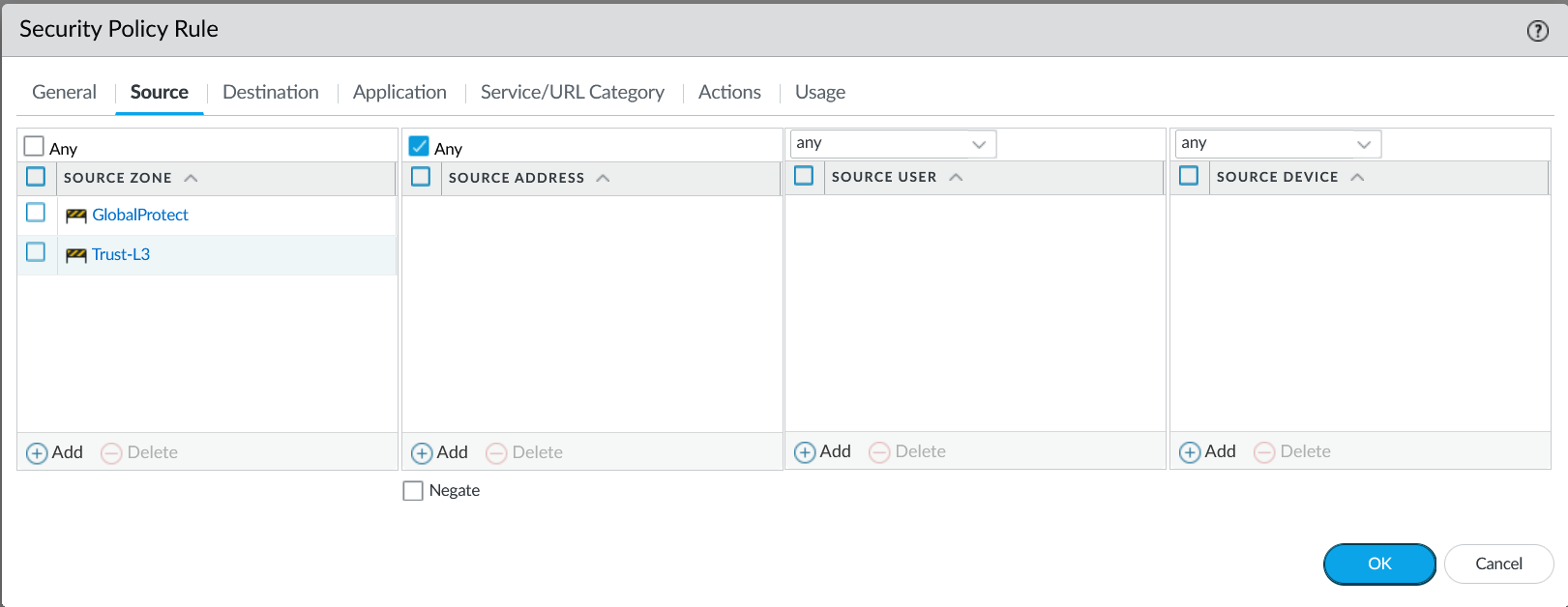
Created a security zone for Global Protect clients.



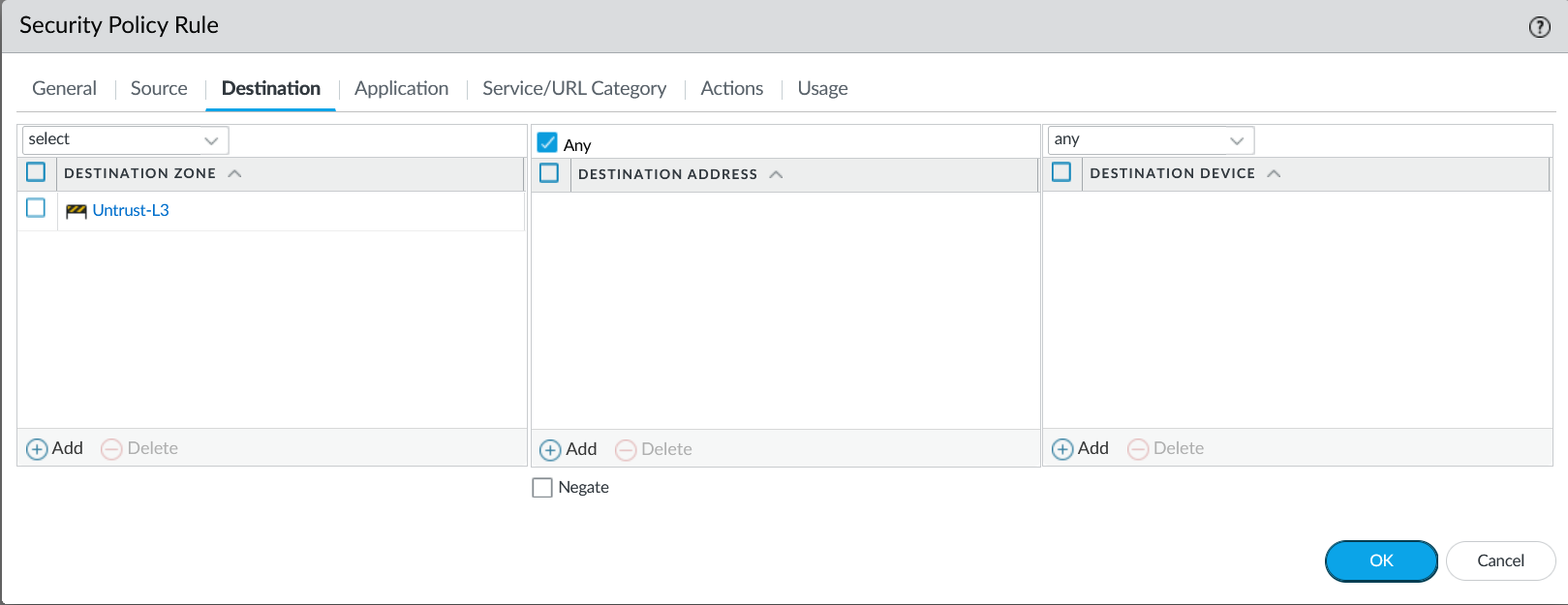
Created a security policy for Global Protect Clients.



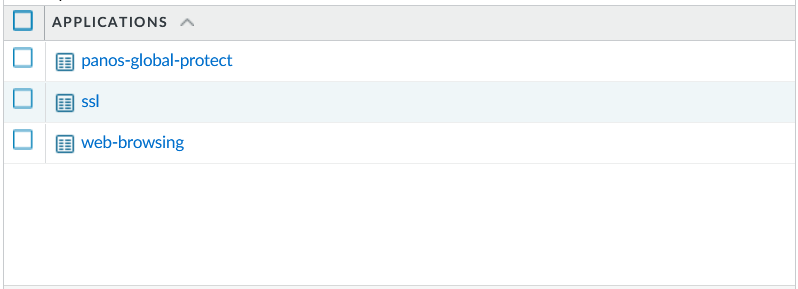
Allows Global Protect traffic as the source.



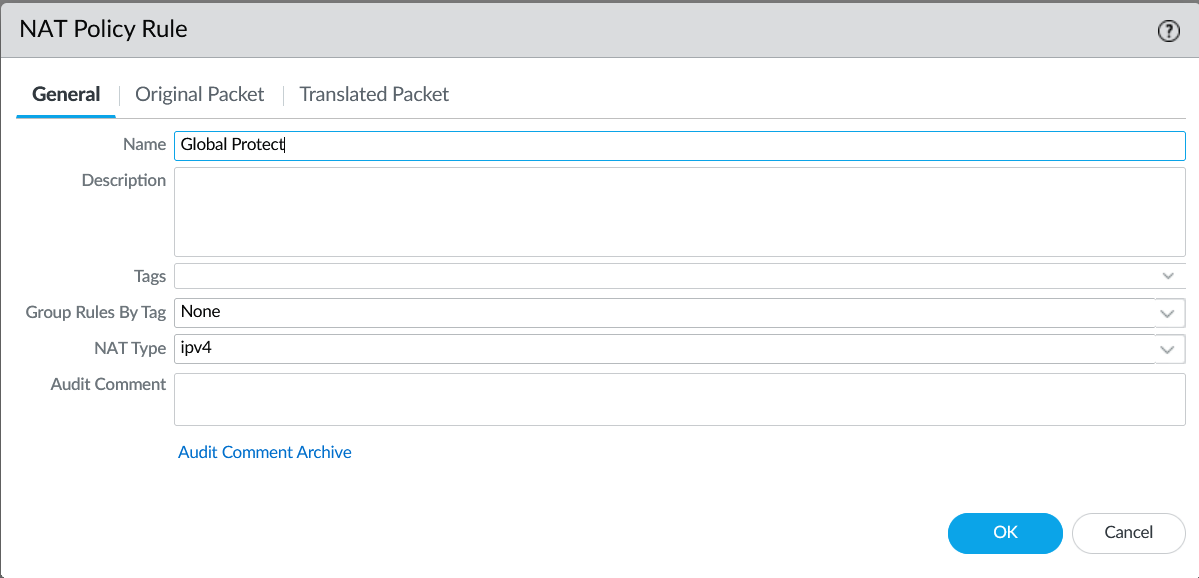
Allows Global Protect traffic to reach the main internet outgoing interface.



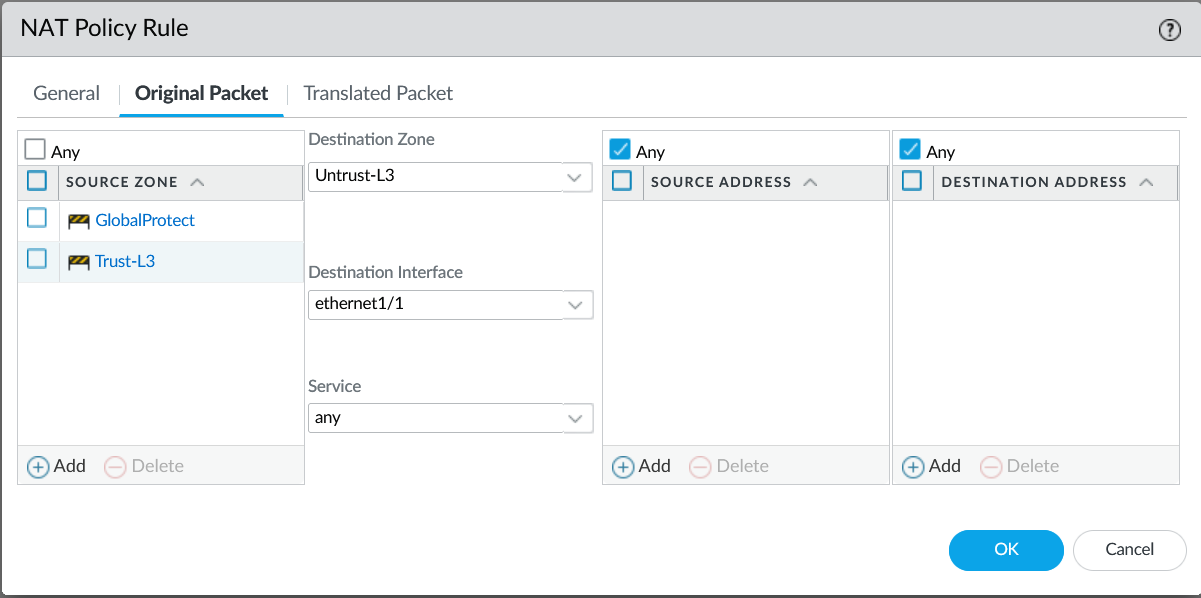
Allows Global Protect, SSL, and Web Browsing.



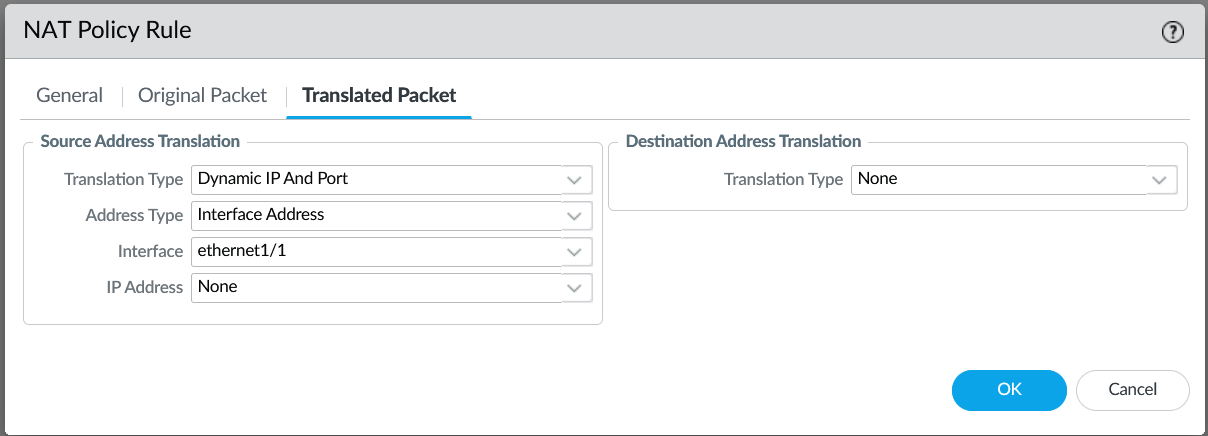
Forwards Global Protect traffic to the internet outgoing interface.



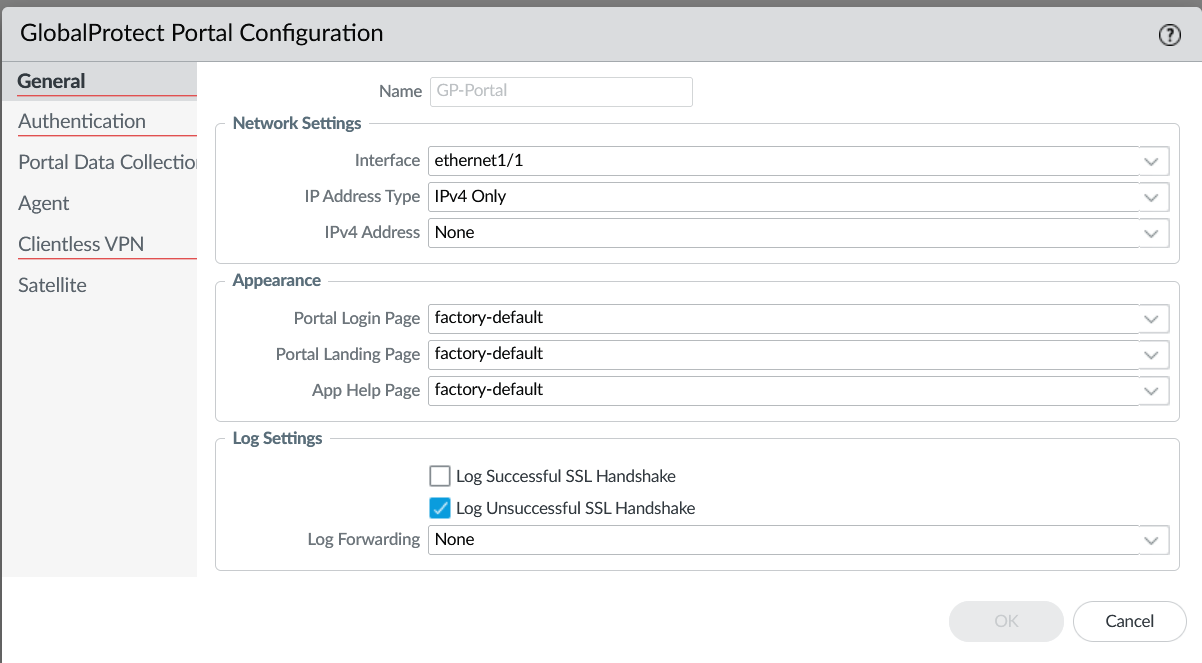
Traffic coming from the trusted layer 3 and Global Protect zone are forwarded to the untrusted security zone and the outside interface.



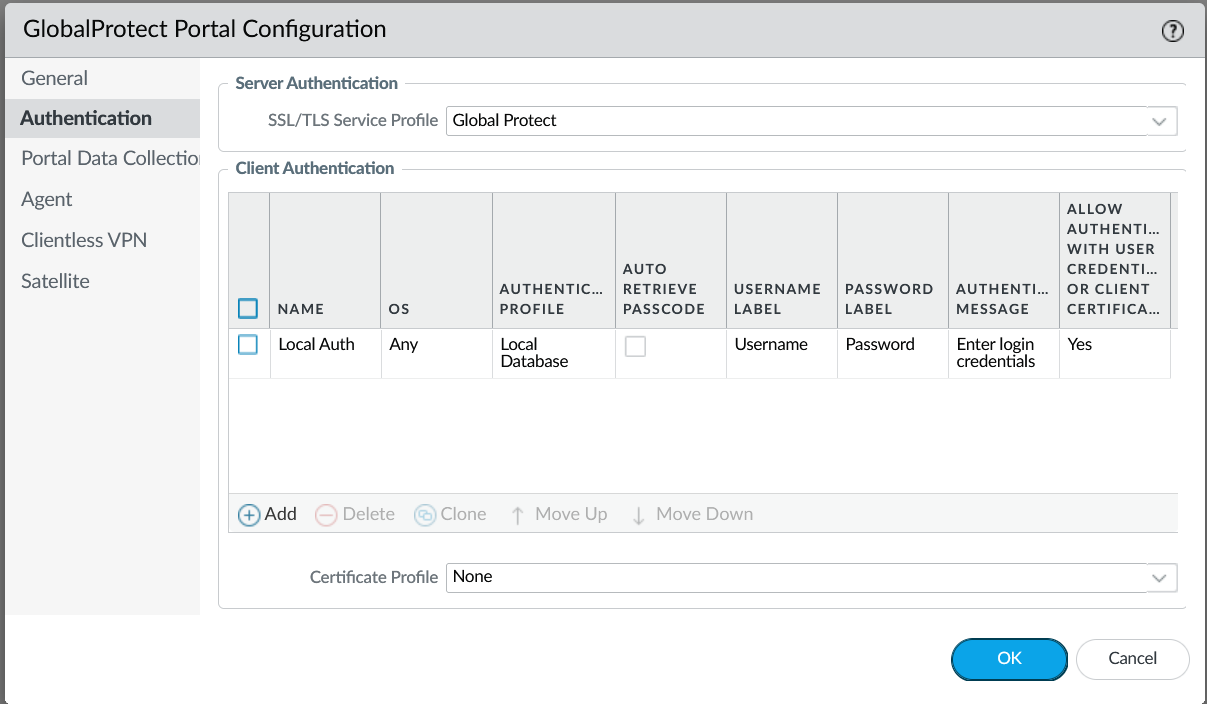
Translates the source addresses of Global Protect to the outside interface.



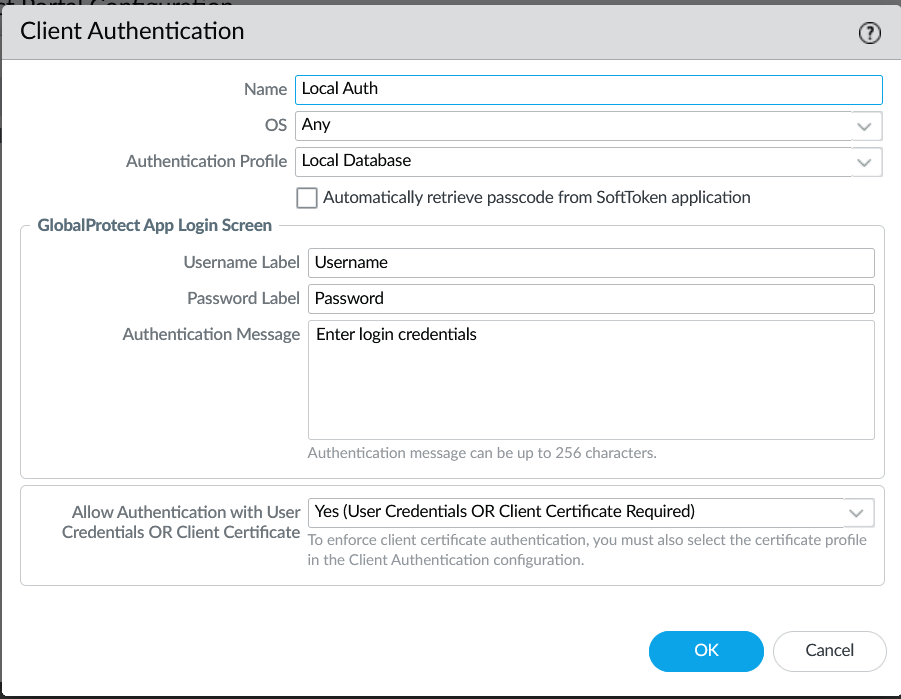
Creating a Portal for Global Protect.



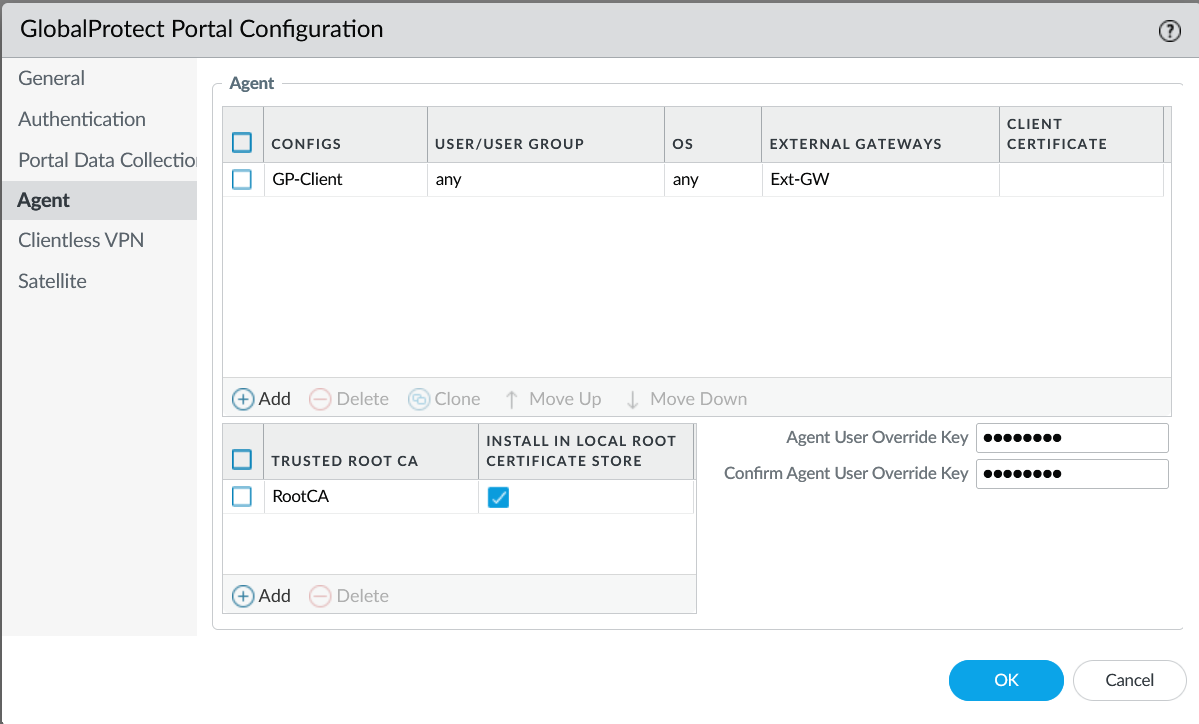
Specifying a SSL/TLS Profile for the Portal to have an HTTPS connection.



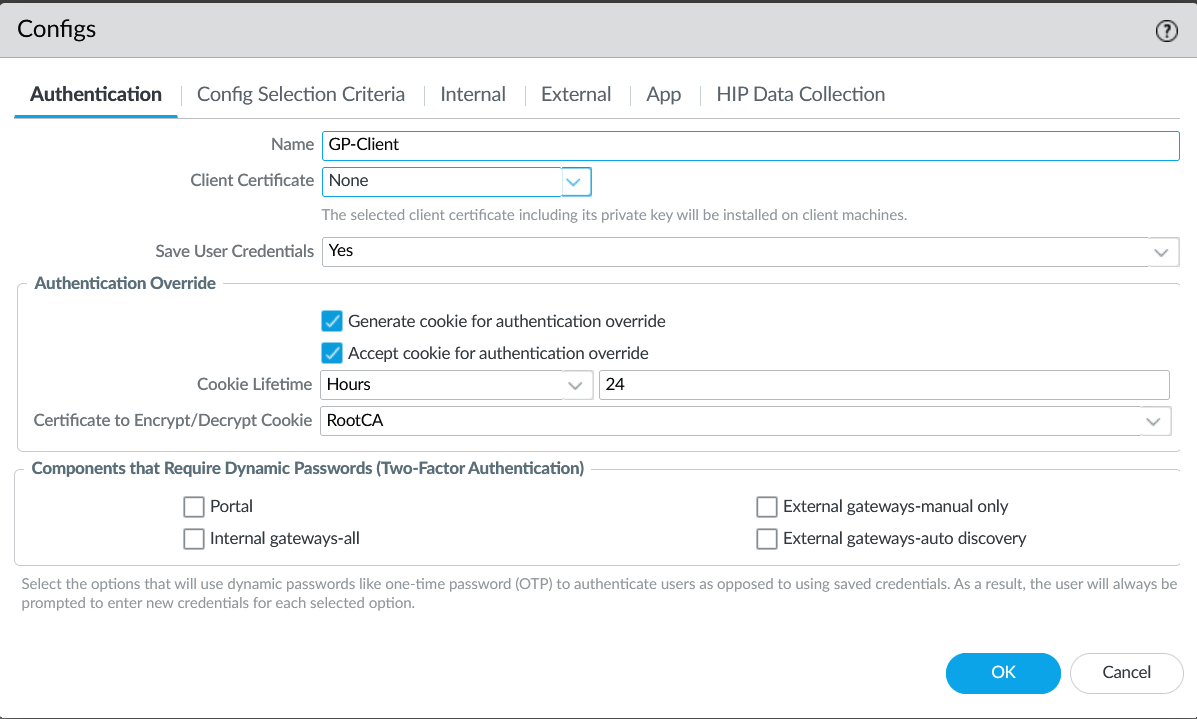
An authentication profile for authenticating local users without needing a certificate.



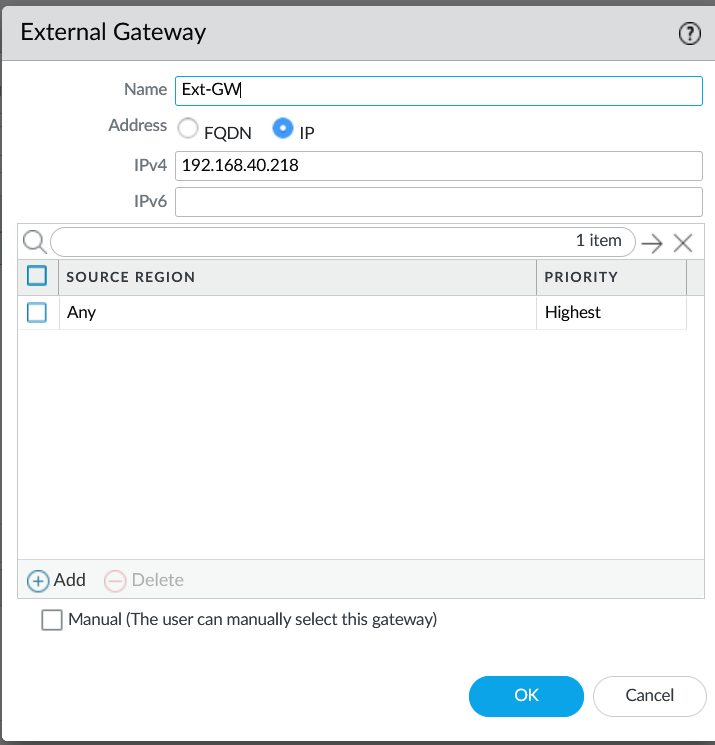
Specifying the Root certificate and a agent profile for the portal.



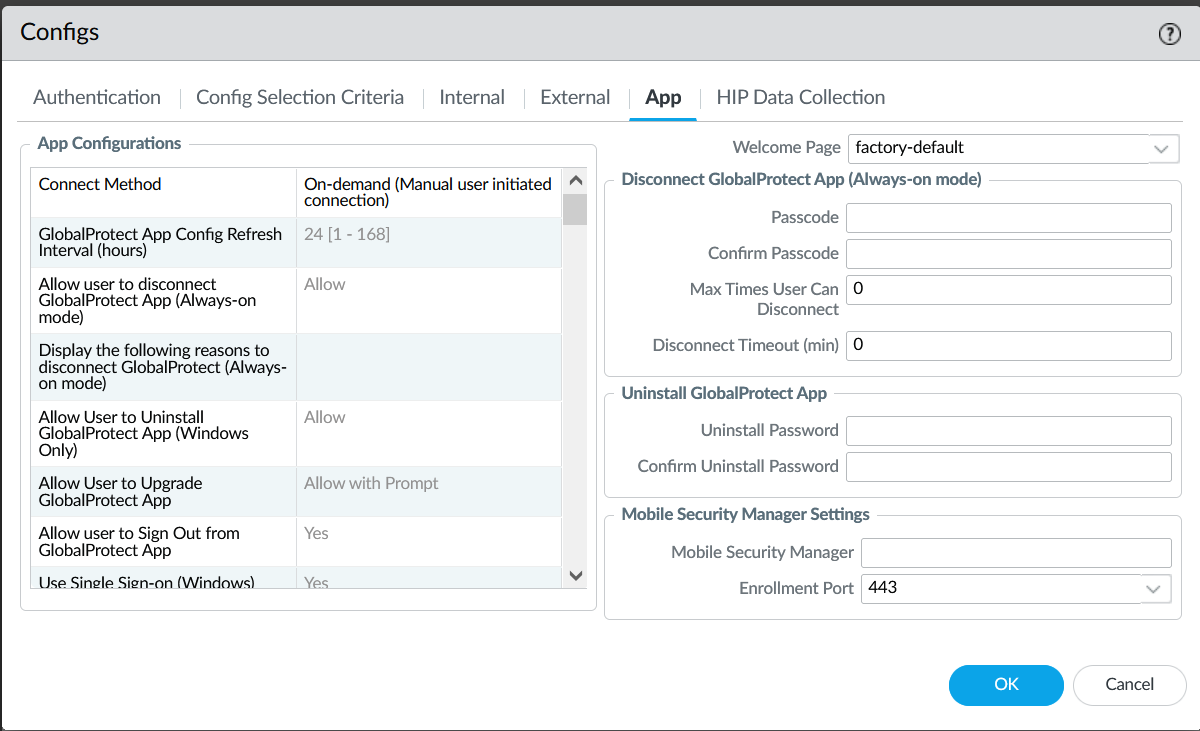
The portal would generate a cookie signed by the root certificate that would be valid for 24 hours, to limit the need to constantly enter login credentials.



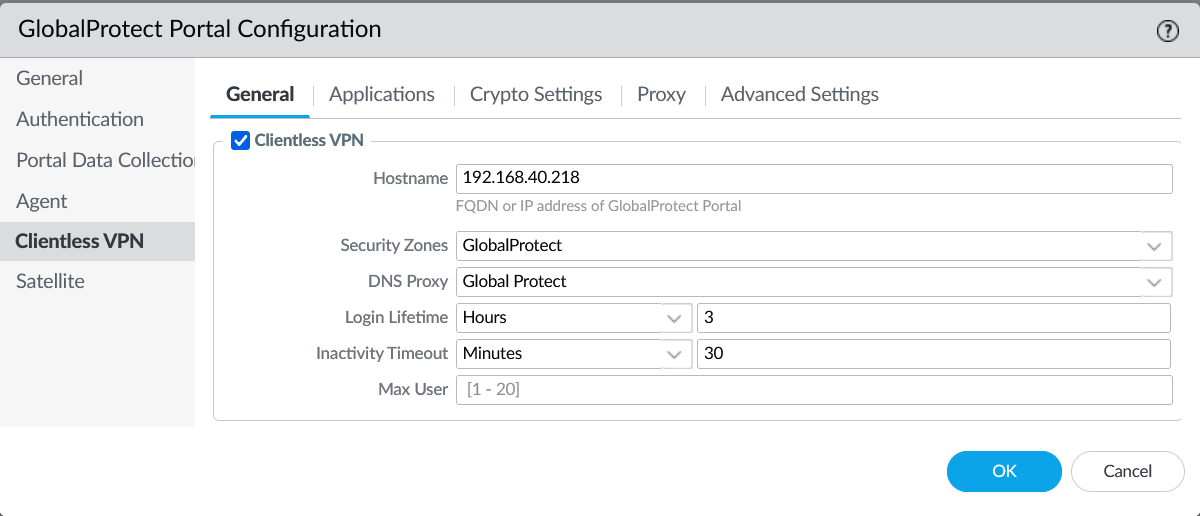
An external gateway that Global Protect clients would connect to.



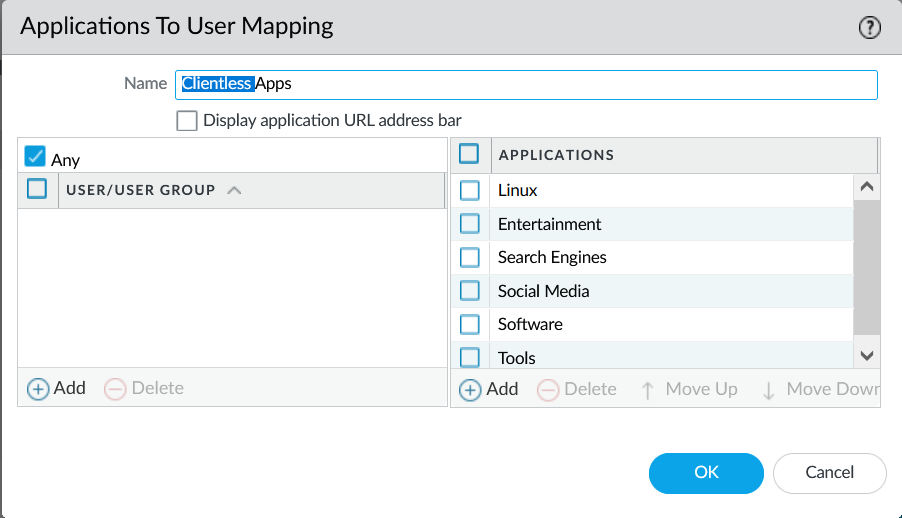
Global Protect would allow connections whenever the user would like to use Global Protect for remote access.



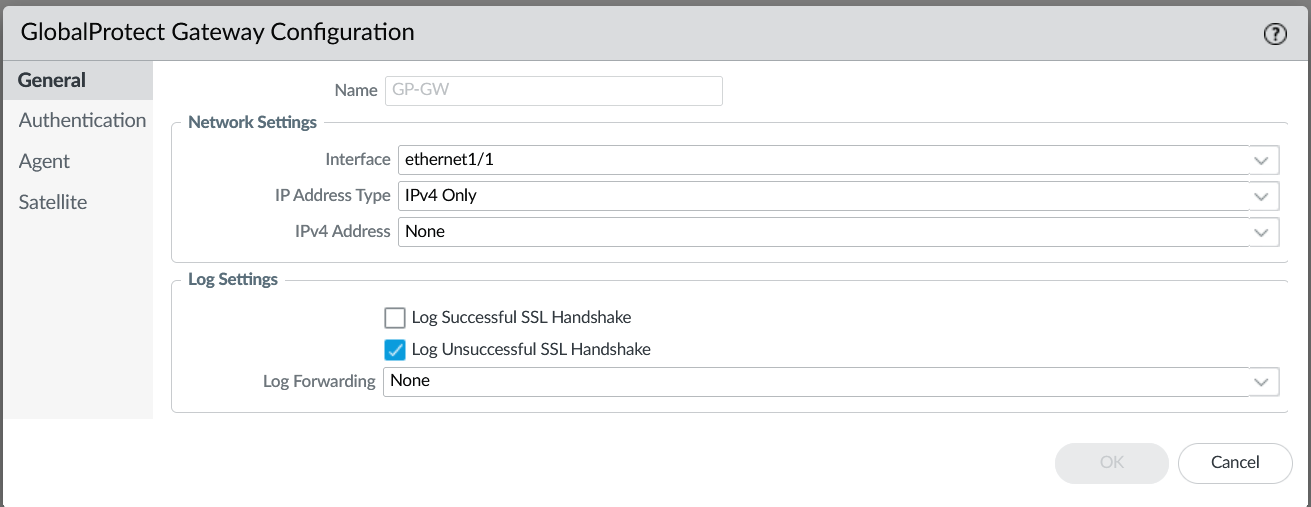
Configuring the portal to allow the user to visit websites without the Global Protect client installed.

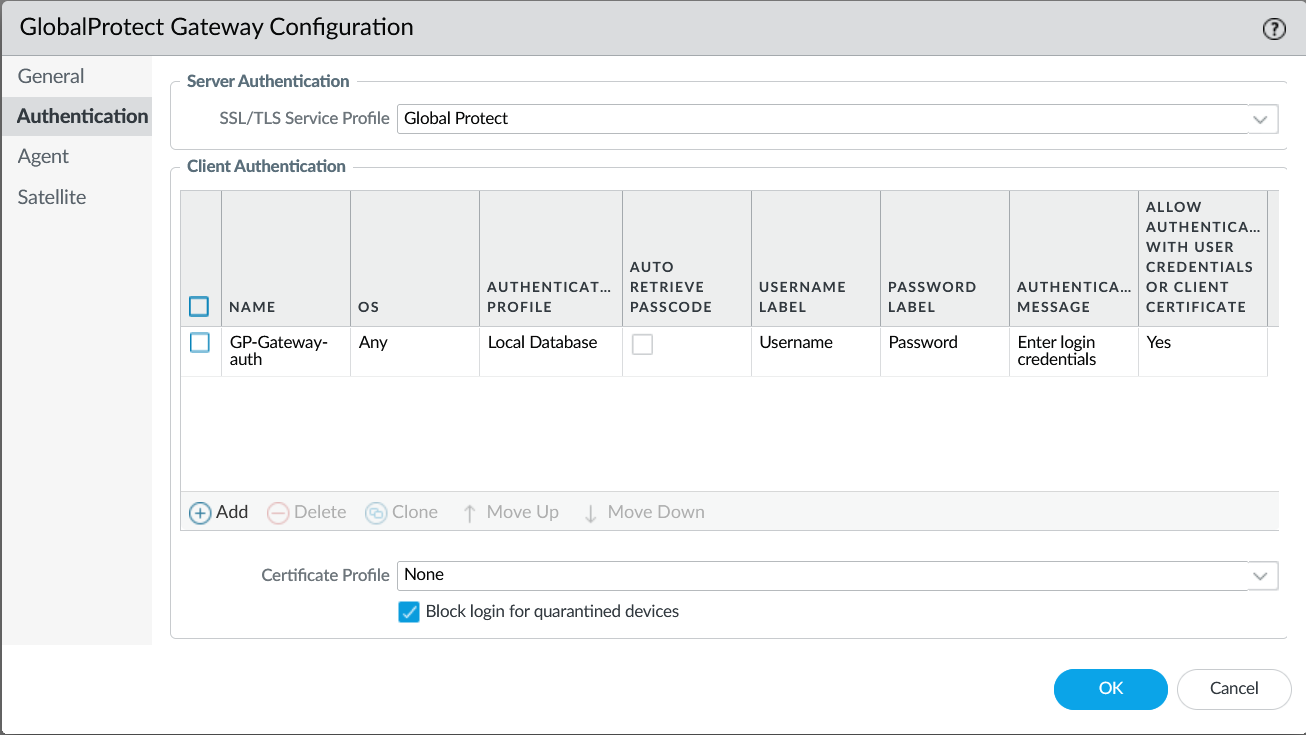


Specifying Apps to appear on the portal when the user logs in through a web browser. In this cases Clientless App groups are specified, so that you would add apps to the groups without needing to sepcify every single app in this menu.

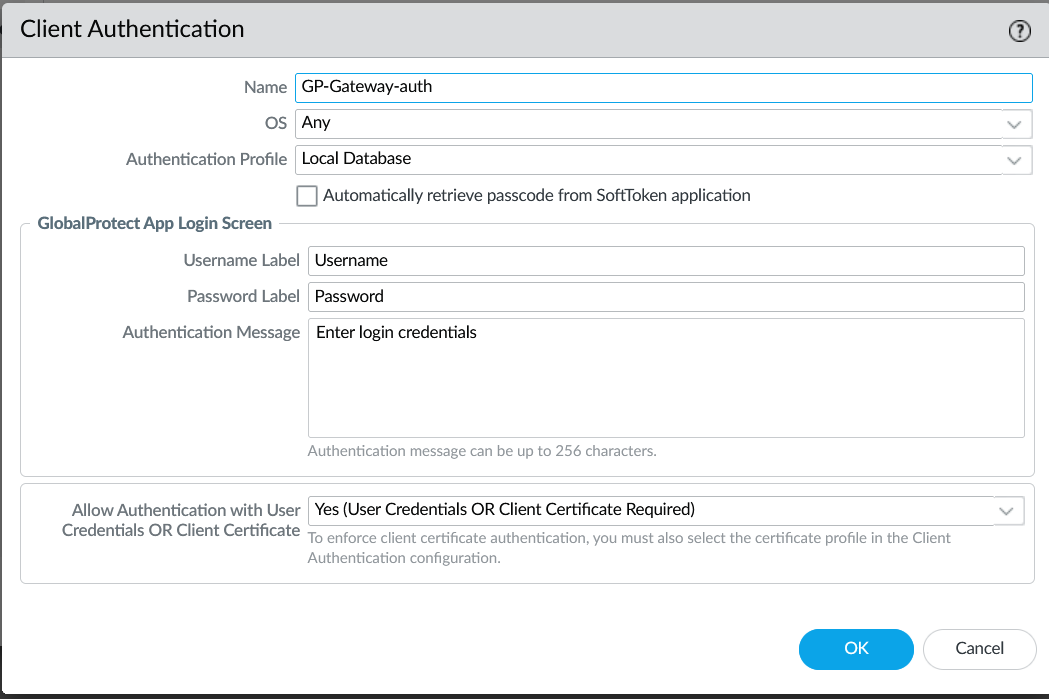


Global Protect Gateway configuration.

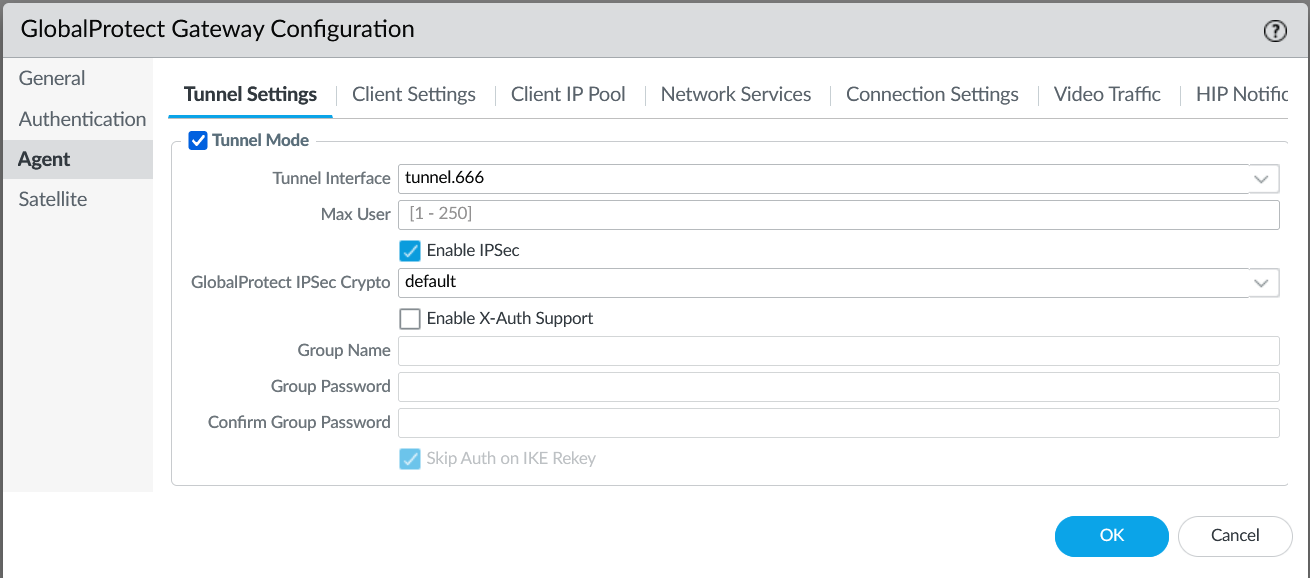




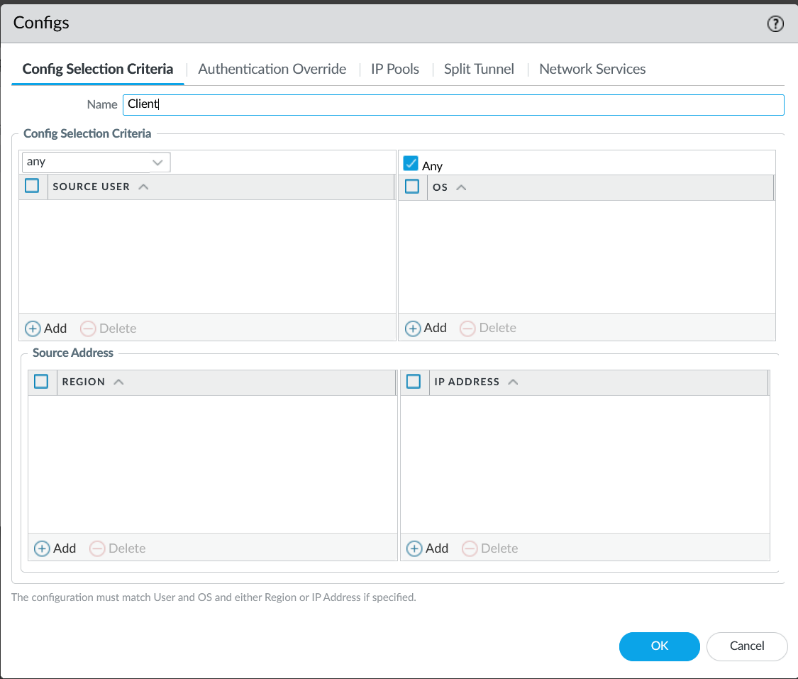
Gateway Authentication configuration



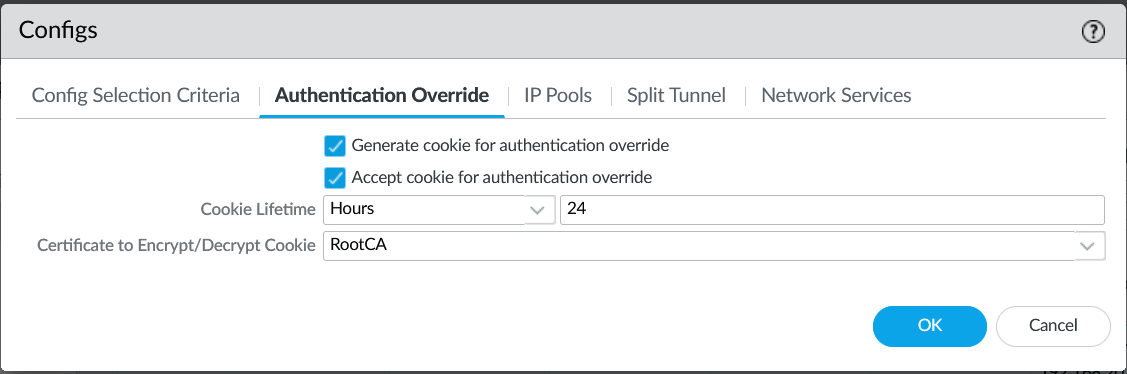
Gateway Agent configuration



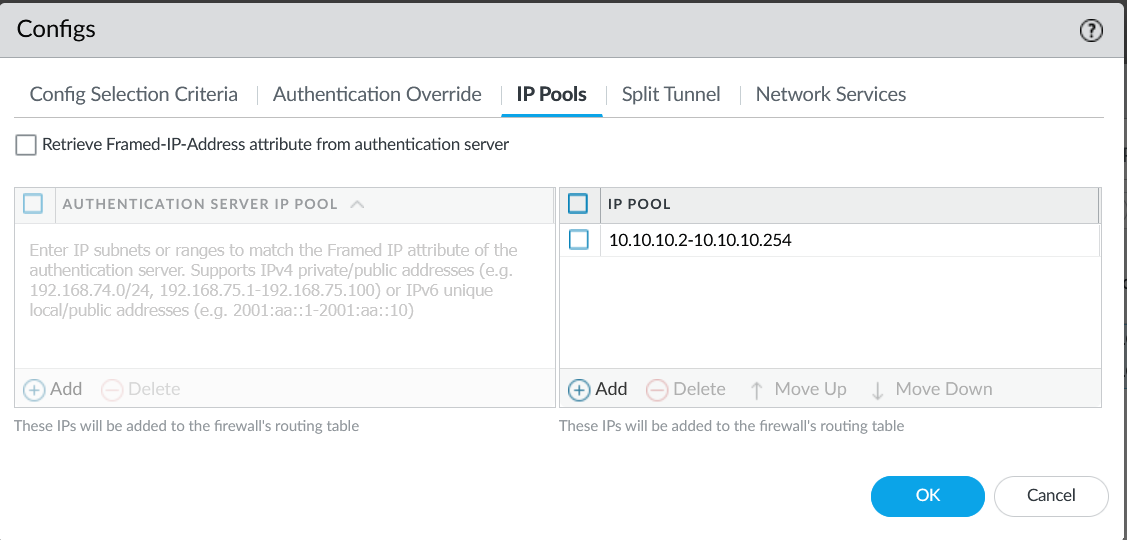
Gateway agent client configuration



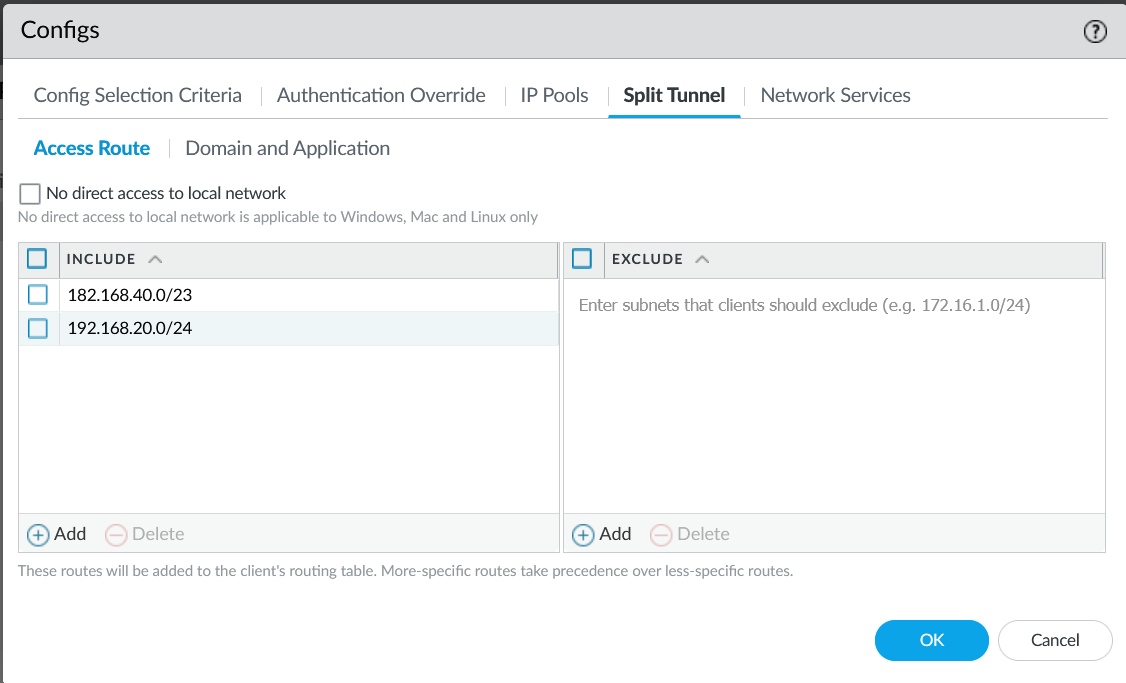
Generates a cookie that would be encrypted by the root certificate, and it would be valid for 24 hours.



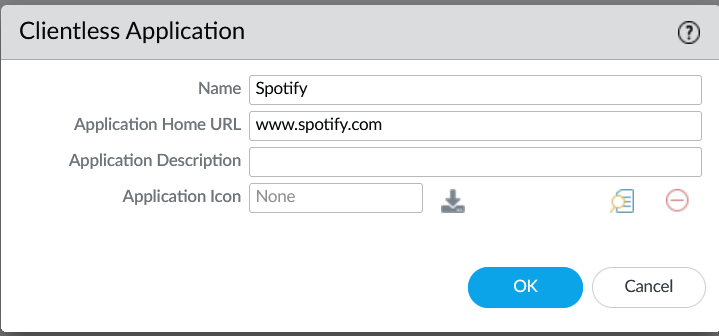
The IP Pool that assigns the clients an ip address that’s available in the address pool.



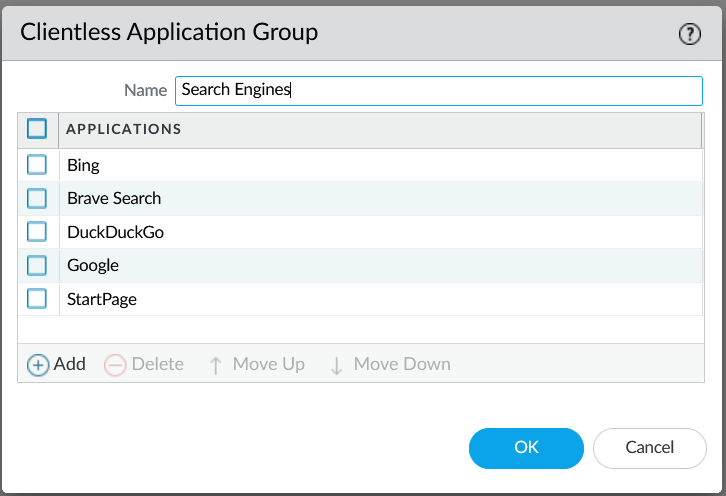
A split tunnel that would give include access to the LAN subnet of the firewall, and the WAN subnet of the internet interface.



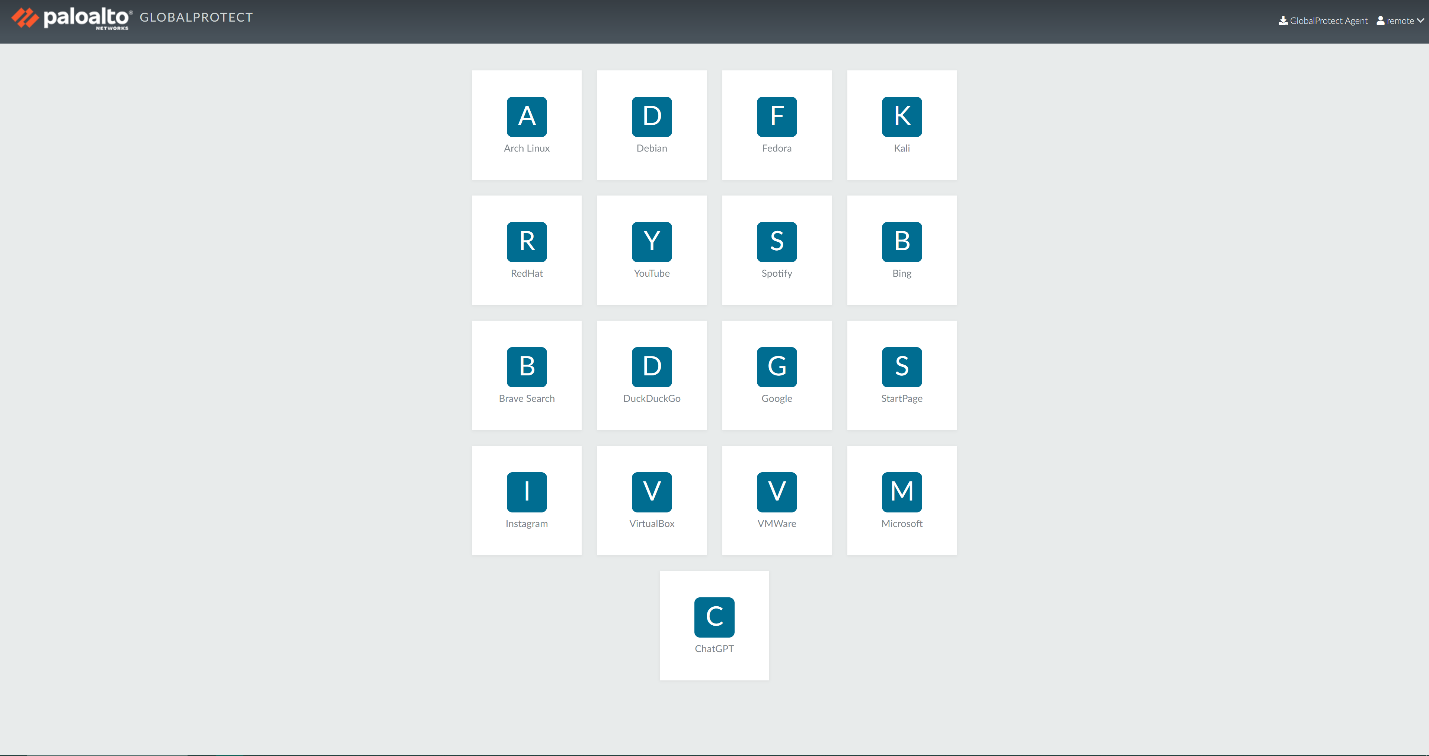
A clientless app that would appear on the portal if the user logged in through a web browser. In this case if the user clicks on this app, it will open Spotify.



A clientless app group that would contain a group of apps, in this case this group contains search engines. This makes it easier to specify the groups in the clientless configuration rather than specifying every single app. In this case.



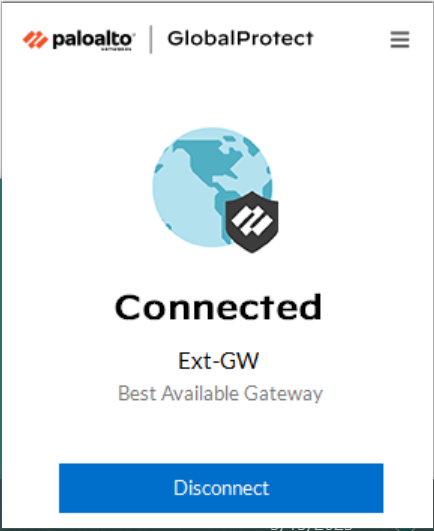
The portal contains clientless apps that the user can visit when they login through a web browser.



The global protect portal without clientless apps configured or if the user wishes to download the global protect client.



The global protect client when the user connects after logging in through the windows client.

****

Problems

We did not encounter any major problems while configuring the lab. But we did encounter some small mistakes that stopped our progress. First, we had an issue where The Global protect client wouldn’t find a reachable gateway, this was fixed by setting the external gateway’s Ip address to the address that was dynamically assigned in the main internet interface. The other problem we faced was that the global protect client would not connect, we found that it was a certificate error and fixed it by making a root certificate, intermediate certificate signed by the root, and a server certificate with the common name being set to the ip address used in Global Protect. When testing Clientless apps on Google search engine and YouTube the websites won’t load and showed that it could not validate data sent to and from those sites.

Conclusion

The objective of the lab was to be able to set up or create a Remote access VPN using Global Protect on a Palo Alto using SSL. During this prosses of configuring the Remote access VPN allowed us to practice and allowed us to familiarize ourselves with Palo Alto Firewall management console and configuring VPN and using SSL. During the lab we encountered some small troubles that we learned from, but we were finally able to create a Palo Alto Remote access VPN with SSL that was able to have users login through a web browser, download a client for user to install locally on their computer and is able to have users visit clientless apps on the portal without needing to install the client onto their computer.