|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | |
|  | | **Palo Alto Remote Access VPNs with Certificates** | | | | |  | |
|  |  | | | | | | |  |
|  | | | |  |  | | | |
|  | | | | 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 Certificates Authentication

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;





;

}

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 abe53d6b;

issuer-hash 0f276ae7;

not-valid-before "May 15 19:51:35 2023 GMT";

issuer GP-VPN-CA;

not-valid-after "May 14 19:51:35 2024 GMT";

common-name remote;

expiry-epoch 1715716295;

ca no;

subject remote;

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

MIIFEDCCAvigAwIBAgIEalFNDzANBgkqhkiG9w0BAQ0FADAUMRIwEAYDVQQDDAlH

UC1WUE4tQ0EwHhcNMjMwNTE1MTk1MTM1WhcNMjQwNTE0MTk1MTM1WjARMQ8wDQYD

VQQDDAZyZW1vdGUwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDe4MqG

vqxueVUsa+mHusVRNCjVQzVJG8H5KQv4Ox6BhbblXGoDbIKOEaZ/bME9ca7m8xfB

Dc81fo31iuM9xlPaVk4AQAI5GDmd55PGMzugnPCoIxQMrxC0RVgBuKIwgDKvY0J2

+fRFFjNWCY3ZZLL7fylY+QC5MBWlyGFEpcLXHFnh/yGPHBHRE2RKDAvZlelwKknD

c+jF6nMZouzjN7ZOU39qGK5mXsxczXpw/4coG4gFbrX19JIplDYnMechKYme14QQ

DieFyGT7GMeYROPC+ve6yS14yJIMb8TNhqTSHtdZVGbfPQ1o2z1RGIQ/I6uvyyPo

r65+Om6PcySD7NEC99SScxY8yssWZjiV7wz3aFrg2RIqD0N2ChtL8zBCvhAObuRz

Exl7bYDmZSFUf13Tvb4Zb9Dlj4Cy36MFjtqpHMdeFGGtgP+5/mhSdTN/NspqzSHu

qp+AJqjDR8vDZuRtVl+kwq7QqVJkUAHqfacVqy/ssOffXk1wkstAFwvi1HfTGrri

5m0rU1PIAhplP9NWBVkfguiSwd9xUhVGdQJ38tr3J5cu9Kd/VxxcxeyoDSF1M5in

Eys3/rqdjjN2lkkiJnCOOPkjhYaGESWfwOOJog9cjF3059bqyh4PuitR+qHz8fvE

2nHMNHFQOFL0b6BHS0xeWc/nlbadxa9iUFcfiQIDAQABo20wazAJBgNVHRMEAjAA

MAsGA1UdDwQEAwIDuDAnBgNVHSUEIDAeBggrBgEFBQcDAQYIKwYBBQUHAwIGCCsG

AQUFBwMFMAkGA1UdIwQCMAAwHQYDVR0OBBYEFE4cDoCcvPKk0ewu8kIjdqS72SFH

MA0GCSqGSIb3DQEBDQUAA4ICAQBXwrXfqERt2Rhrwsx/pXnwaZafsZuV0NxeoXuE

OfzcjurZdnLn1iSxHyQUwPRc5NkPtfHk4o9WqTDw9tau1VOUEFQLr5nfHqihsRHA

8oZIkFmiD0c4FpuYq08YjoJp/VRyPc+7D9HJt0tbqjQle5y5eYQq9AgkHss4qE8f

4/oAmqrO5Wg/dpmQ6BhwZooamo5F+zAelZk/7gtbTog4KfX0YfCz567RATofVy4U

UPMvMVqtGJHi42CL3wuz+Ygea1ZFtQZy/VjSt5E/LZhpArEIMJTDtgobcwdd9qeG

hbbgo7GNPm7TPDxg+v2S8W5T09hWzj9QoOI8BjUpzMz8ePSUhSA5sMRsFJAb4zqT

g8S5wgJDO3wajepB7X6Ia06SwmqP5RqcLhql1+FQuTg0wSgz157F128Is9yKttld

po1eX9tPi7EBJW2GmxSMYoOGFt1jSSkUufLnKodphVscF7Gvs+9OsPyOdAd3DSU4

DfEVMbH3Eq7gMfRRwK1NUi937K5TSXx8VT9R0fPUWLIVh5/YGW60OCIKyfKDfjlv

XBykm8SGyhCnpyTeIb+DWjo/AILubHxTEJ02PYmWhr4pi7AXjpI6WbEZBqRc0kv/

5l6FYRPJhgN5iCa3+j8nlTsEDYm0jQ1ogR8yKmw+Tt/Qd0IynlsGowZWdntWNCwJ

CvMAhg==

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

";

algorithm RSA;

private-key -AQ==/6fhNOGOoqtQEYO8N4sExUqEyUo=



;

}

GP-VPN-Server {

subject-hash 719dc427;

issuer-hash 0f276ae7;

not-valid-before "May 25 14:12:50 2023 GMT";

issuer GP-VPN-CA;

not-valid-after "May 24 14:12:50 2024 GMT";

common-name 192.168.40.164;

expiry-epoch 1716559970;

ca no;

subject 192.168.40.164;

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

MIIFGDCCAwCgAwIBAgIEalFNFjANBgkqhkiG9w0BAQ0FADAUMRIwEAYDVQQDDAlH

UC1WUE4tQ0EwHhcNMjMwNTI1MTQxMjUwWhcNMjQwNTI0MTQxMjUwWjAZMRcwFQYD

VQQDDA4xOTIuMTY4LjQwLjE2NDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoC

ggIBAOcbsbFO8XFvntB2YMgezzZ/FNXJnwPaeVaqe11+moxVzP0iUhjxqNSy5kWK

hWu/Wizk6ScagO2oBV6JMzHwv+Sn2qG6g3pT2oRLWvt/HPU7oUUpvSJlidUoSd7w

jWDdz2FEiYvM0lYPnfYFmqayzeNetzfFLaajbu0ssw8vkXyDtVkR7ZlcqGgIlOG0

UfFiNvDecjVeJTXRW6I6Qfglj/XMTzDbyacvildBiIx+kczvn24pkat01oKWpnbS

ssvhh8JBVD9UMw8pVr0+988usNeLH/0sMQBJZT/mxUWap92GQYy4bCYM831jg+XH

H9YrDgpvv+4Zlv+jfG2FgGDyvL1P+glcI0wKaNMsXOG7p08C4jPeBO43cRofY4ez

A7RHAe9LSJs8y5HFnno5+GMO3SUvsc5fMQ95MQHXSDW+1qejDbnfbaUReX4gmAKG

szZ+LrN0ybC3IXqmw1DY9WxRVdRRt6JbiBdHMLRkigxUyd+OdbKHvjuCo5Dqmsuz

gZZBDNxuJF2DCWQVyJc/RqKhUAboDgBpVFqjyeL/HiWRkKUjGR3NcoqEt7+N15Ci

BWWKIMKPdu6wdxWe231zq9mspuP3ujrIfQvO5ItKi1ilK55fiFc8YuhzBxrEwJ+0

JSb6fMPo6gObmhajiGyH0CGUezMfIfXOvG+qXgOEYS1wXmirAgMBAAGjbTBrMAkG

A1UdEwQCMAAwCwYDVR0PBAQDAgO4MCcGA1UdJQQgMB4GCCsGAQUFBwMBBggrBgEF

BQcDAgYIKwYBBQUHAwUwCQYDVR0jBAIwADAdBgNVHQ4EFgQUuYi01jj5QOoddA0l

LCQeyX96zyUwDQYJKoZIhvcNAQENBQADggIBANQmqN/QpuGtiSgzYVWnI3DtGFio

QoUZbSHBnA1gjtrSM9Eus1aspGVOchEqyMWww50oeW07RzrfPqhLXInPq99RcLhm

SzE+1kKwdOuREp9m4xhUCN4K8/VDdRBB8mF6GDkKdjxFQca3uDarcSqL49USaxUQ

59SrZSA9NtzMjCiA03AOBwd0GGRWQ6Q+iqJZqFEjSXN5GJHOP/1J/uNNIkvD56vF

9pjwB7qcX7Xvilu0K4Sf7+8MEeaRnkImE7fSjVoQXCLEiodIn2q/P3Dos2Qndfio

5wP/hicVm413laBanr3DZxEk91eZwhGWB/BcNXzWt4dkot0Zw1sSFO3BzjeuSEAd

n9gu3lumDSr+nOK6/w3uBBA7LtHx3QXHabdR6BrSUHPLsHtvwghXdlSks8sGIprr

ptv1BIh0Cfx2H4F++whEldqeYmEwVm2R4JpyWQvxFi5QVZ6F494JG6U5OJPdeCor

sS6ivPMc4yQQoGXfoPB5skkGJR4DNsS9SomZfjx3RhhQ2NwBcr9PLzgOHsJ4cZ3k

ks6Bg3ZdxN6Ofqrc000AJ6hssSpE2qSpAGu281YiRHhzF4Tr8ZofFCkDoatmDArL

7Gu3dA9/xNUZ8SmyjjyS5HL/b7vp3LX83jqTrWAt/ioNpzIoi7Yd8e/flvgWAAjn

2puBWEquItcpKjyB

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

";

algorithm RSA;

private-key -AQ==FBn6wsKhOYZYHZjVMyOiy0K1wGA=wfL5Zc+wUAak+B7CnAVY6NdutYWtt67XvF+yGHFGS+uZlDK3xAPOdeBmnOosOHj3wX5Bm4UpzZl0xe3aXnmEM77L516hSfowMRm6CKiliZgi/oTVH8V7tonyRHwcFyewV7kskbQ3flKcJS1DJaS+1splKUv/gIlWrlqZknD3SPfRossw3XW5L3+IQkggb6FCxrtSccEXgYnfk18Ic5a3CJvzHvmcHpDFGttHYHXz9xLYg+XlJhV867POKLfEswMwjOt8EfPTWqVajYJzQOMIi5pCcK2q+K89F1





AmkzsWtLcwhW+kDaBJKiISDIjDSq8d+QqS4fn1ogym44DyaoUO/7H4JY0gNNh4Oo=;

}

}

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;

}

}

}

content-preview;

}

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 {

weekly {

at 08:30;

day-of-week monday;

action download-and-install;

}

}

}

global-protect-clientless-vpn {

recurring {

weekly {

at 08:30;

day-of-week monday;

action download-and-install;

}

}

}

global-protect-datafile {

recurring {

weekly {

at 08:30;

day-of-week monday;

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";

profile-setting {

group Internet;

}

}

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

to [ Trust-L3 Untrust-L3];

from GlobalProtect;

source any;

destination any;

source-user any;

category any;

application any;

service application-default;

source-hip any;

destination-hip any;

action allow;

profile-setting {

group Internet;

}

}

}

}

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;

source any;

destination any;

service any;

to-interface ethernet1/1;

}

"GlobalProtect Internal" 5d949575-bd80-44fe-91fb-9dd66763607e {

source-translation {

dynamic-ip-and-port {

interface-address {

ip 192.168.20.1/24;

interface vlan.666;

}

}

}

to Trust-L3;

from GlobalProtect;

source any;

destination any;

service any;

description "Forwards GlobalProtect traffic to the management network.";

to-interface vlan.666;

}

}

}

}

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 {

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;

certificate-profile GlobalProtect;

client-auth {

"Portal Authentication" {

user-credential-or-client-cert-required no;

os Any;

authentication-profile "Local Database";

authentication-message "Enter login credentials";

auto-retrieve-passcode no;

username-label Username;

password-label Password;

}

}

}

client-config {

configs {

GP-Client {

hip-collection {

max-wait-time 20;

collect-hip-data yes;

}

gateways {

external {

list {

Ext-GW {

ip {

ipv4 192.168.40.164;

}

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;

}

client-certificate {

local GP-VPN-Client;

}

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 {

Protect 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 your 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;

}

GP-VPN-CA {

install-in-cert-store no;

}

}

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 192.168.40.164;

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 {

"Gateway Authentication" {

os Any;

authentication-profile "Local Database";

authentication-message "Enter login credentials";

user-credential-or-client-cert-required no;

auto-retrieve-passcode no;

username-label Username;

password-label Password;

}

}

remote-user-tunnel-configs {

Client {

split-tunneling {

include-domains {

list;

}

exclude-domains {

list;

}

access-route 0.0.0.0/0;

exclude-access-route;

include-applications;

exclude-applications;

}

authentication-override {

accept-cookie {

cookie-lifetime {

lifetime-in-hours 24;

}

}

cookie-encrypt-decrypt-cert RootCA;

generate-cookie yes;

}

source-address {

ip-address;

region;

}

source-user any;

authentication-server-ip-pool;

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;

certificate-profile GlobalProtect;

}

}

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;

}

"PA Web Console" {

application-home-url <https://192.168.20.10>;

}

}

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 "PA Web Console"];

}

"Social Media" {

members Instagram;

}

}

}

}

}

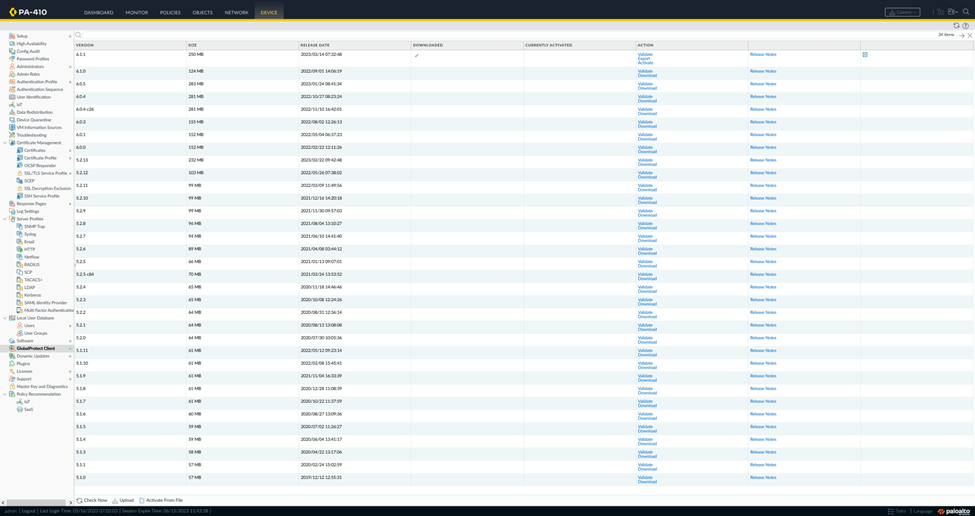
}

}

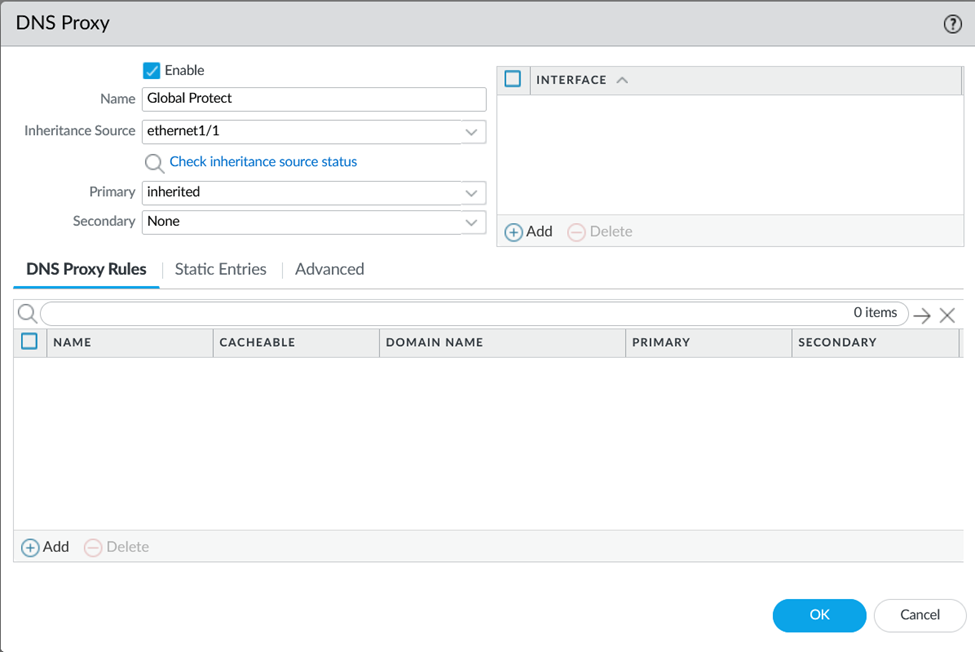
}

Screenshots

Activating Palo Alto Client.



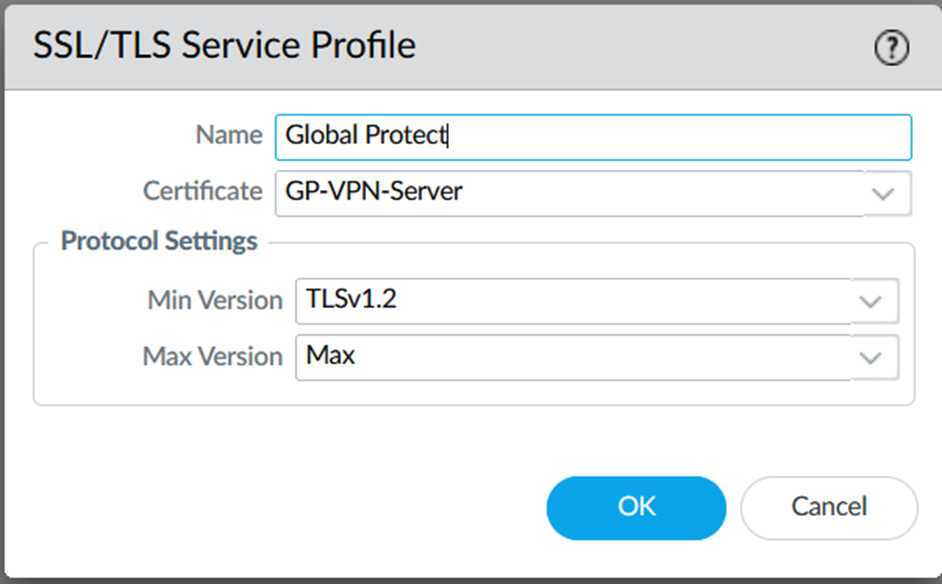
Created DNS Proxy profile for clientless apps.



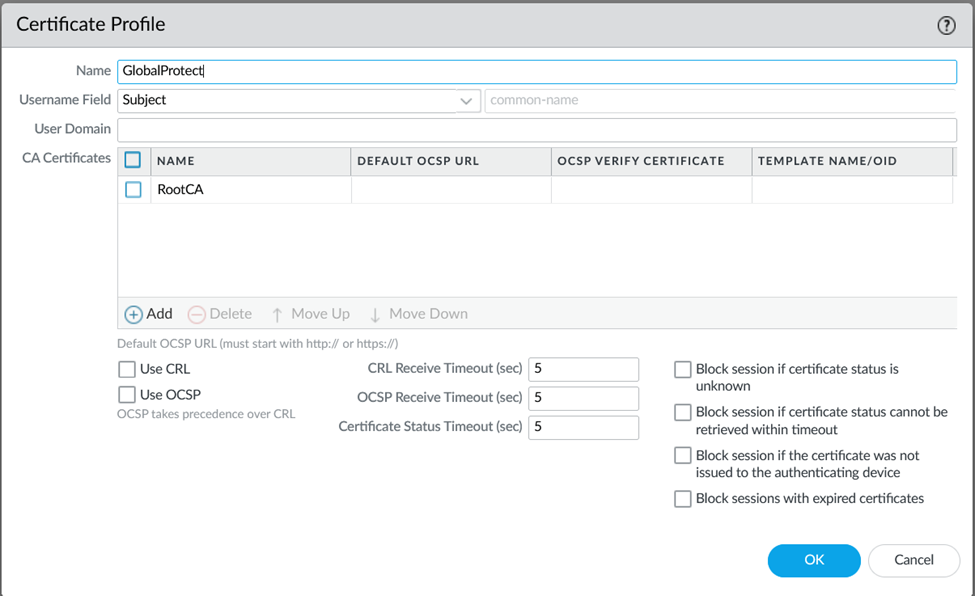
Generated Root CA, Intermediate CA, and Server certificate. The client certificate is for certificate authentication.



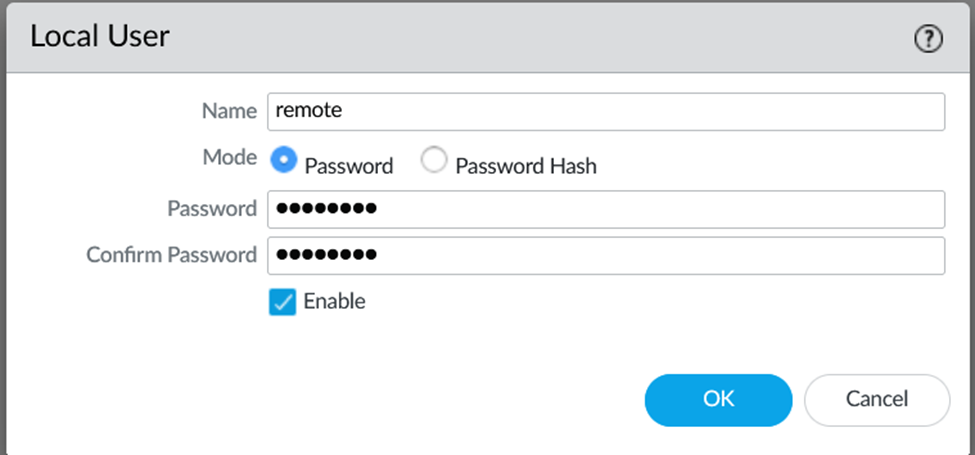
SSL/TLS Profile for the Global Protect portal.



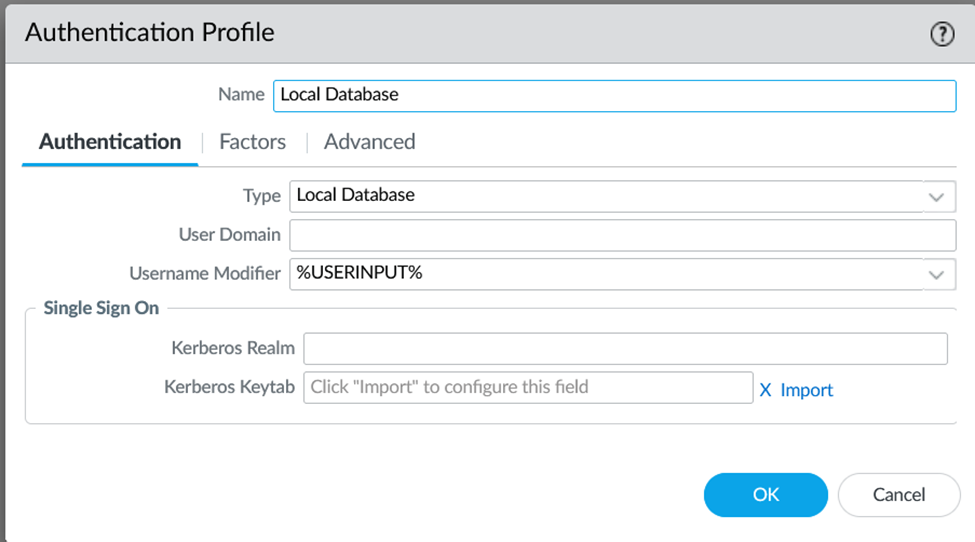
Certificate Profile for Certificate authentication.



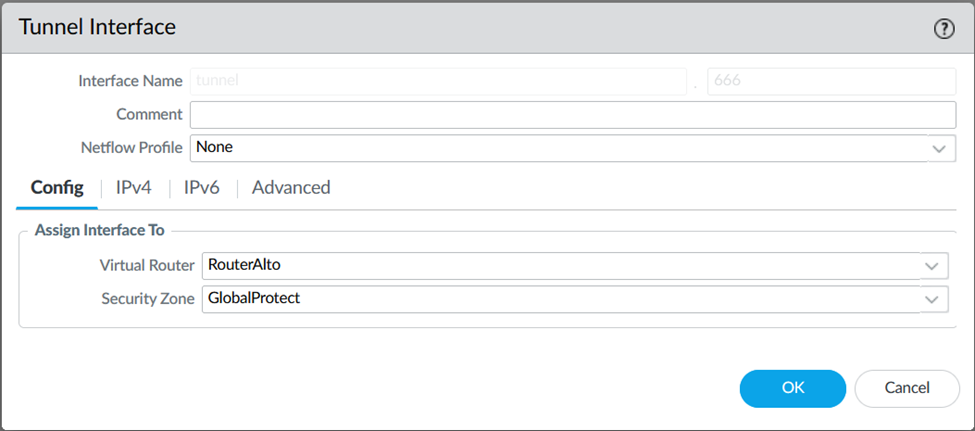
Created a local user that is used for local user authentication.



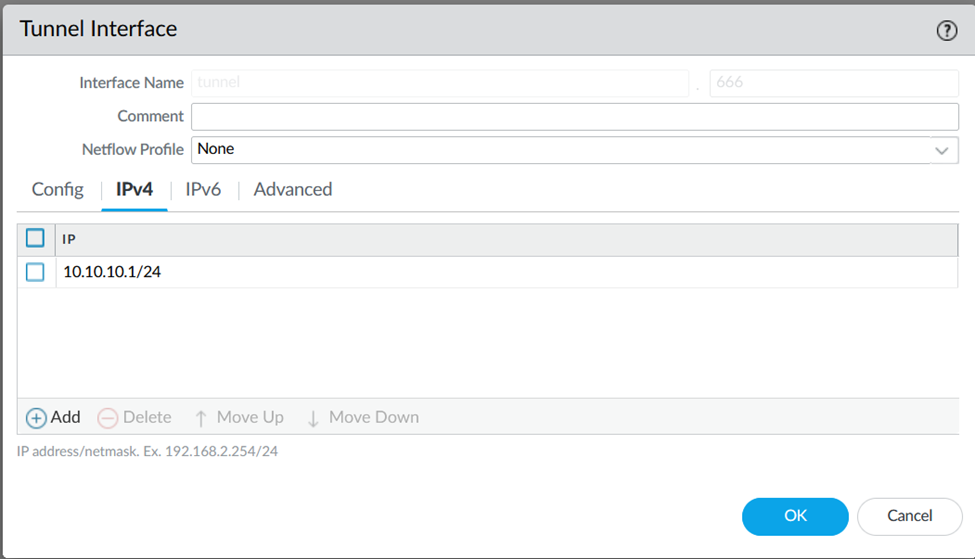
Authentication profile for Global protect to authenticate local users.



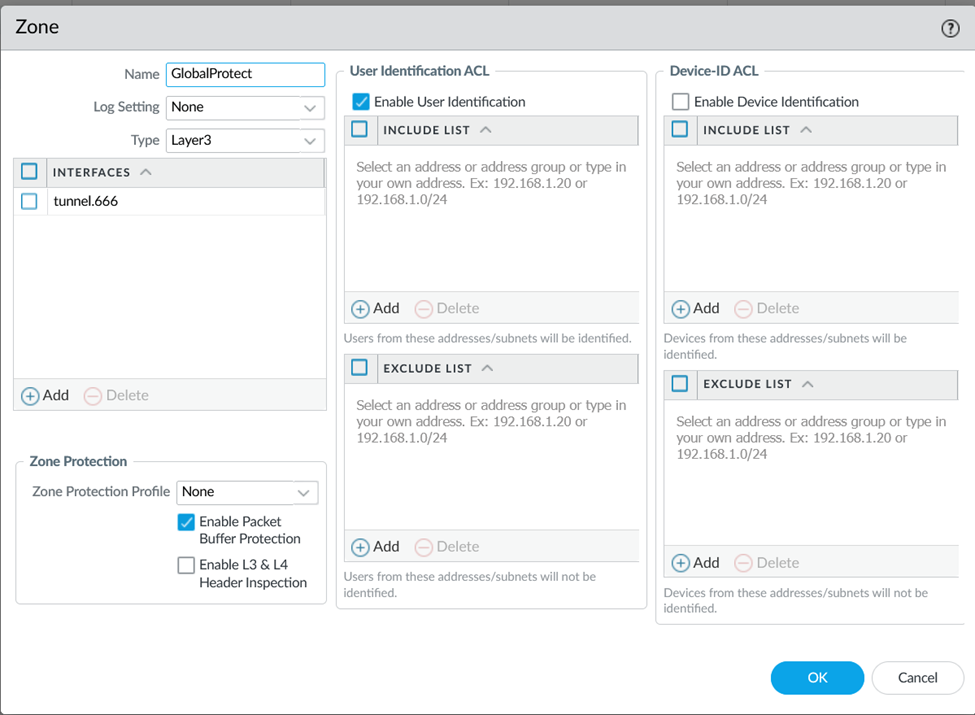
Tunnel interface for the Global Protect portal.



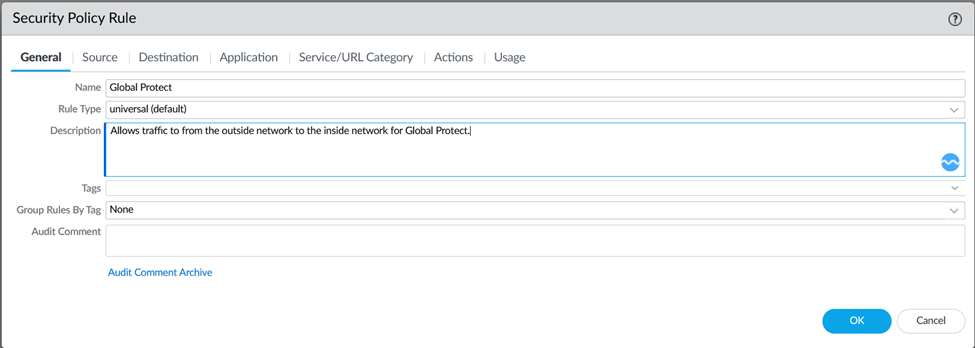
Configured an IPv4 address for the tunnel interface, even though it’s not required it still works with an IP address assigned to the tunnel interface.



Created a security zone for Global Protect clients.

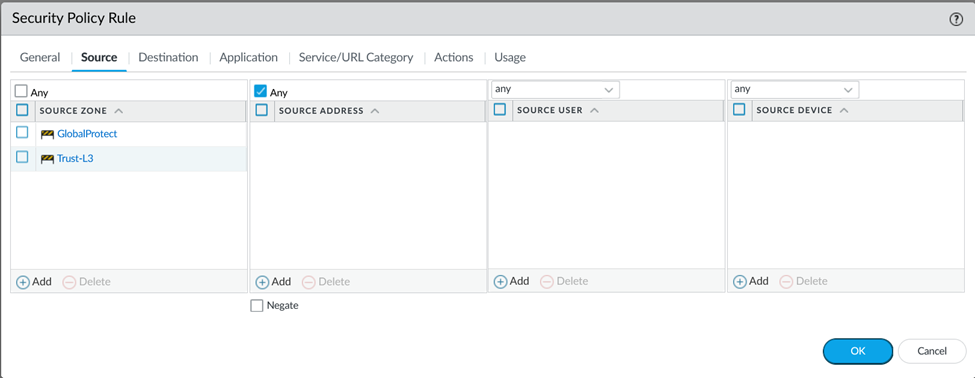


Created a security policy for Global Protect Clients.



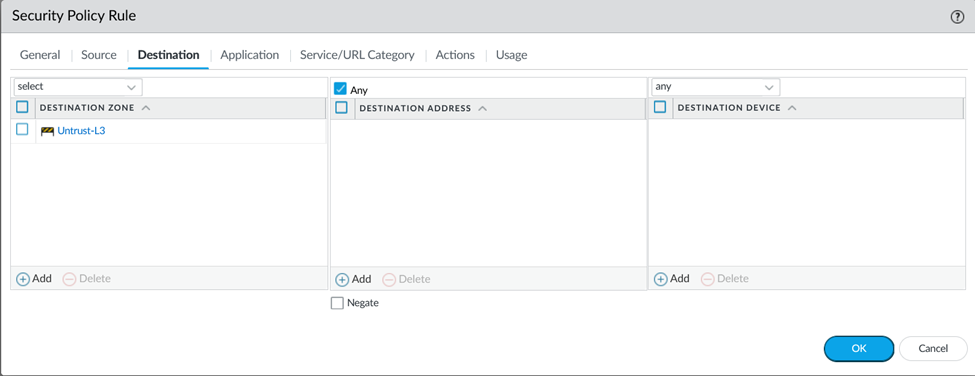
Allows Global Protect traffic as the source.

**Fix:**  Removed “Trust-L3” from source zones.

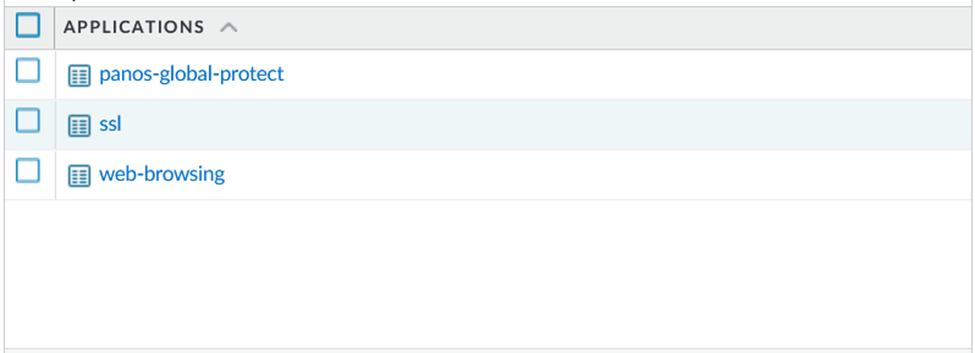


Allows Global Protect traffic to reach the main internet outgoing interface.

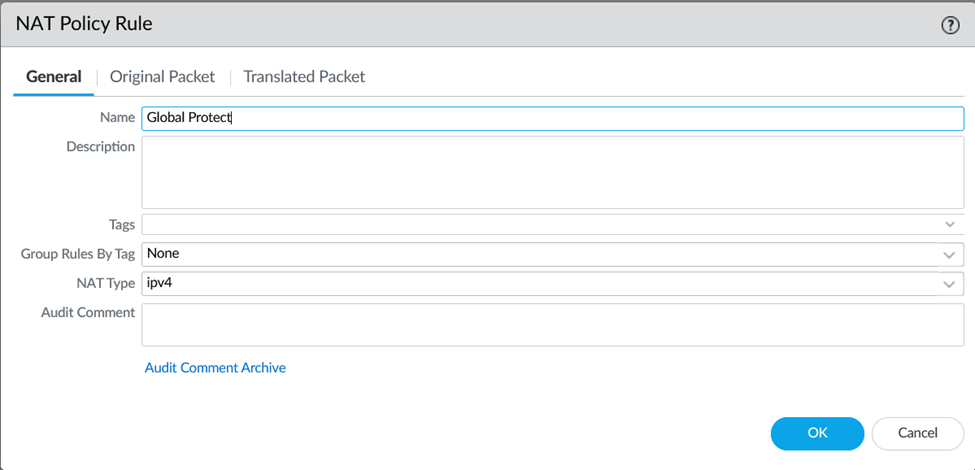
**Fix:** Added “Trust-L3” to allow traffic into the internal network.



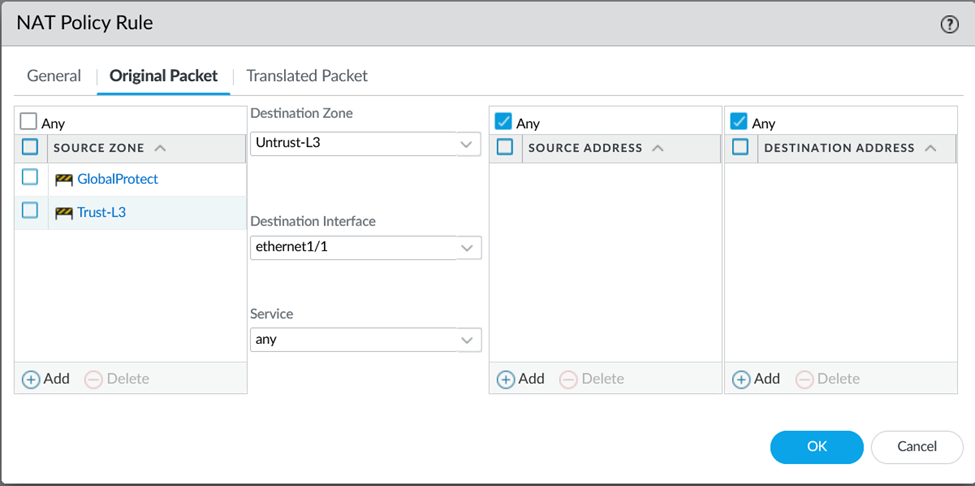
Allows Global Protect, SSL, and Web Browsing.



Global Protect traffic to the internet outgoing interface.

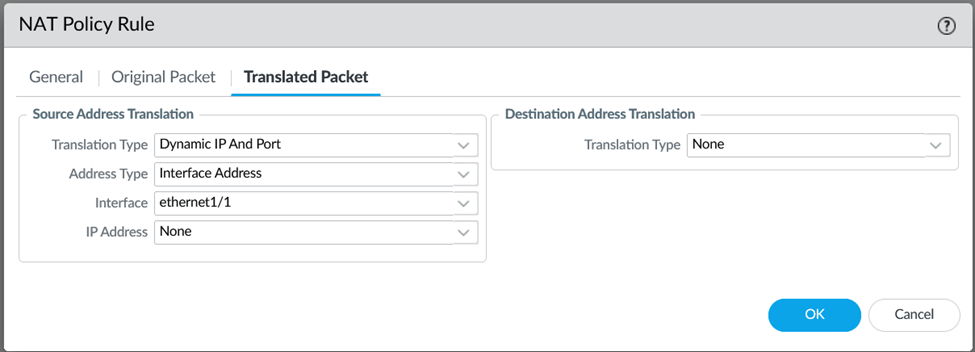


Traffic coming from the trusted layer 3 and Global Protect zone are forwarded to the untrusted security zone and the outside interface.

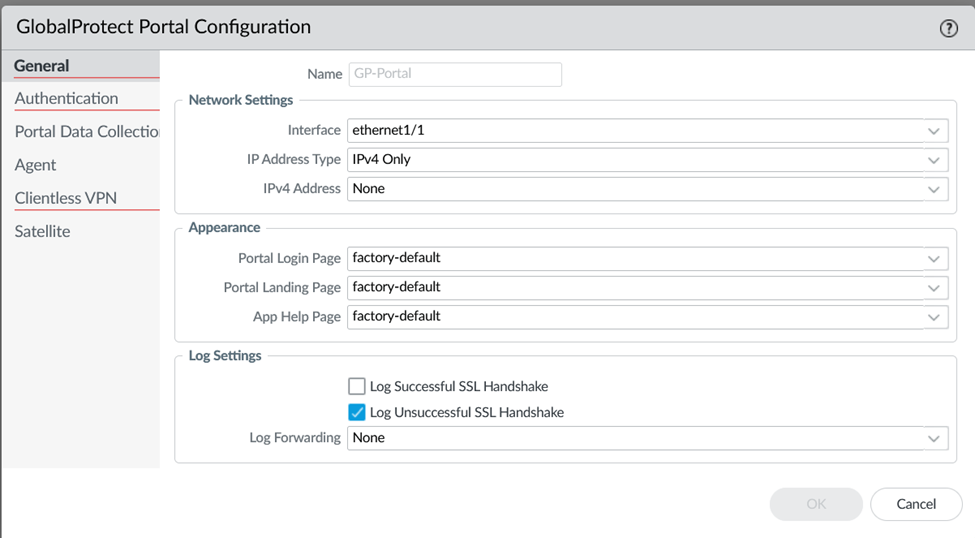


Translates the source addresses of Global Protect to the outside interface.

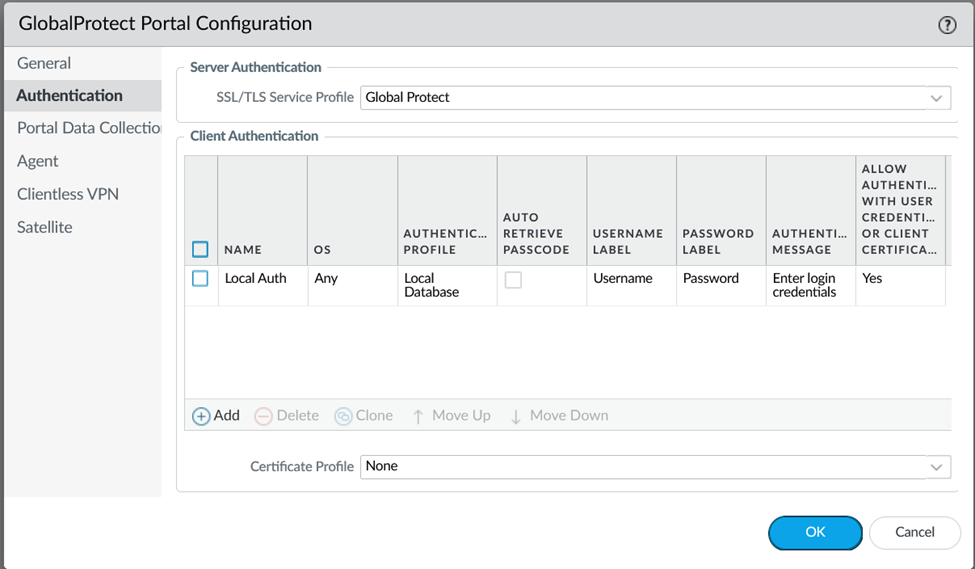
**Fix:** Created another NAT policy that would forward any traffic meant for the internal network to be forwarded to “vlan.666”.



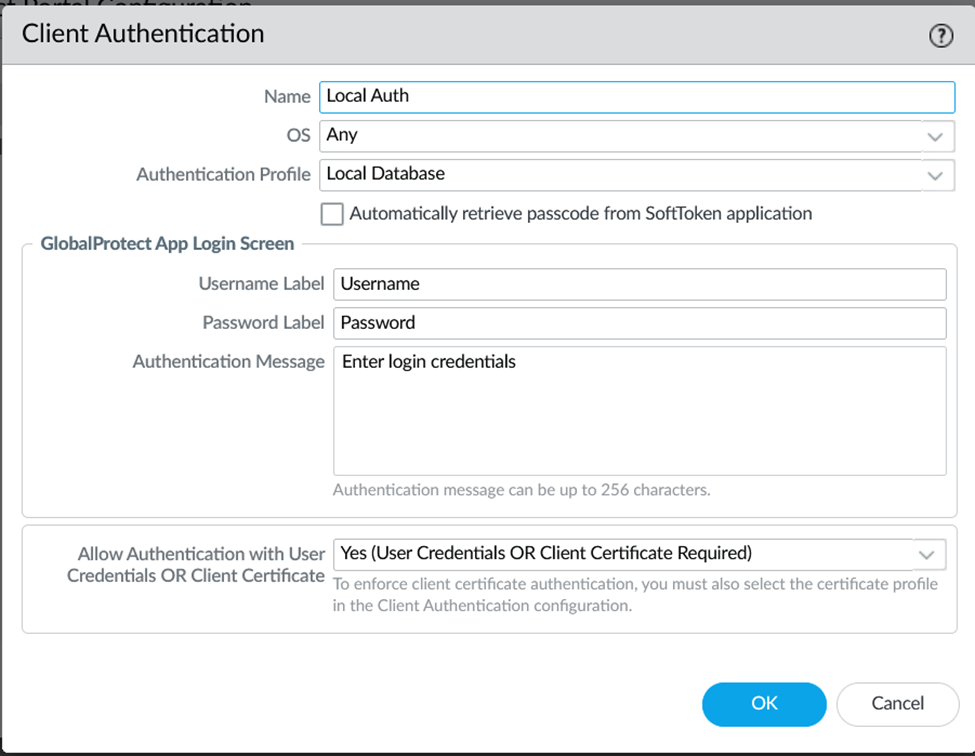
Creating a Portal for Global Protect.



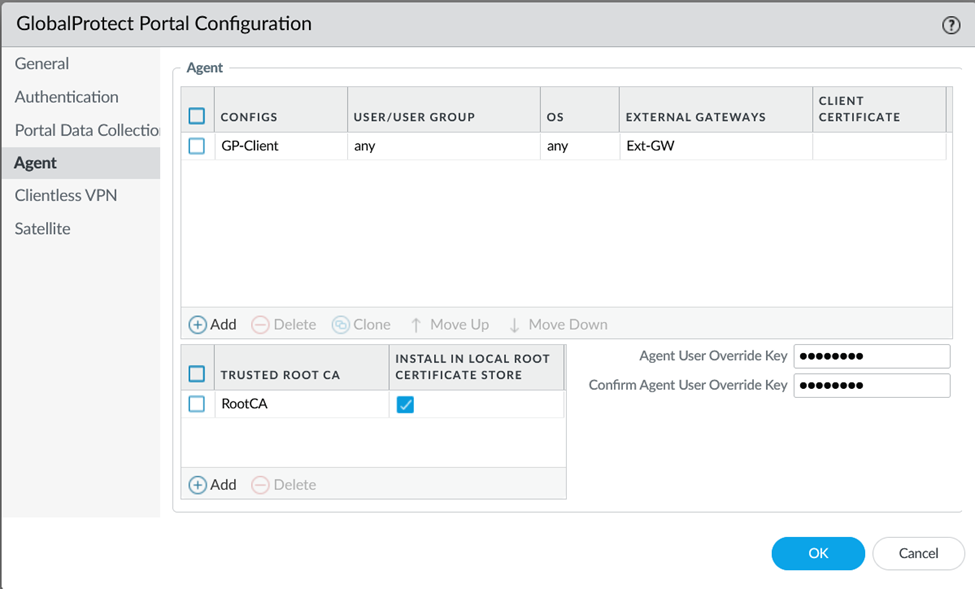
Specifying a SSL/TLS Profile for the Portal to have an HTTPS connection.



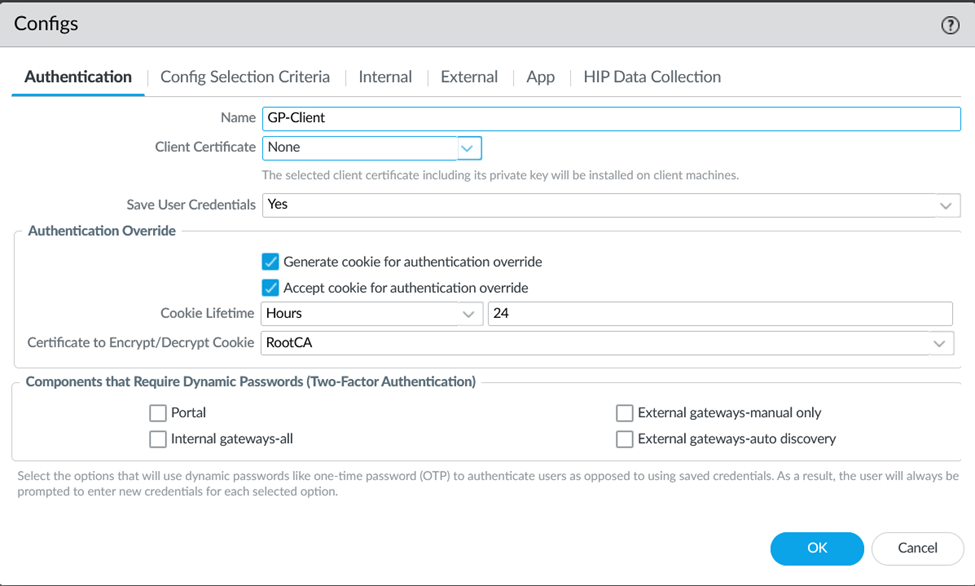
An authentication profile for authenticating local users without needing a certificate.



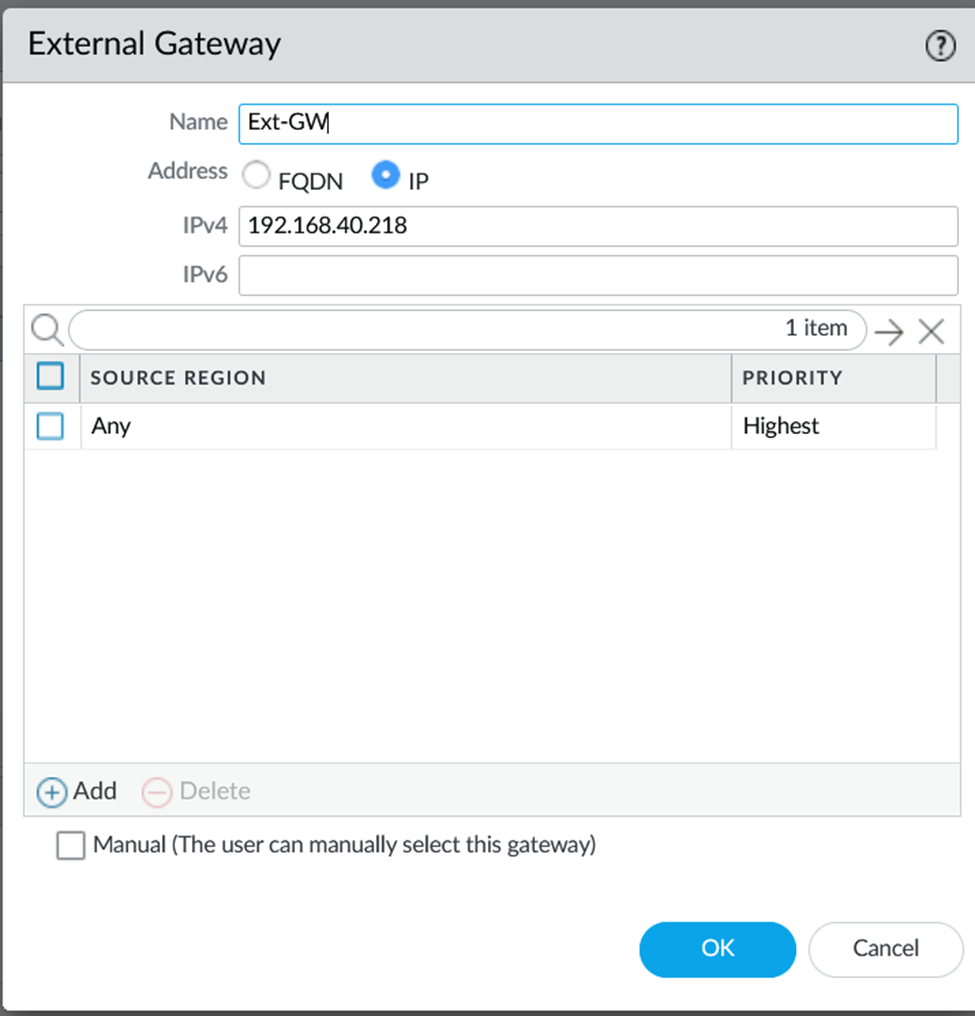
Specifying the Root certificate and a agent profile for the portal.



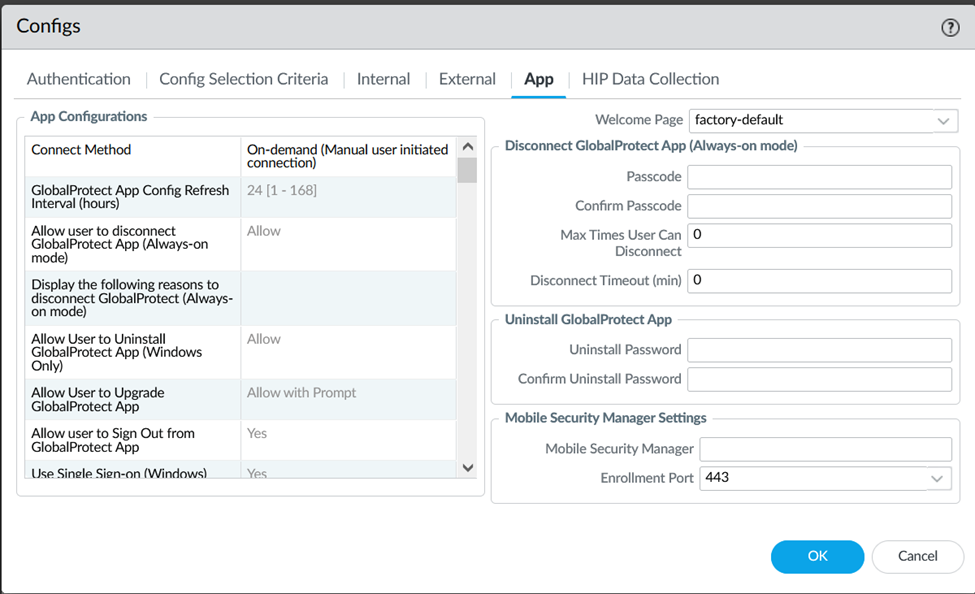
The portal would generate a cookie signed by the root certificate that would be valid for 24 hours, to limit the need to constantly enter login credentials.



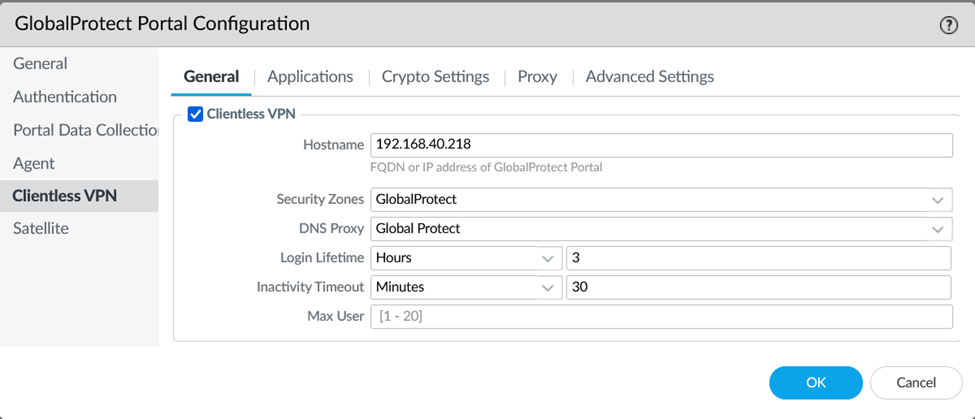
An external gateway that Global Protect clients would connect to.



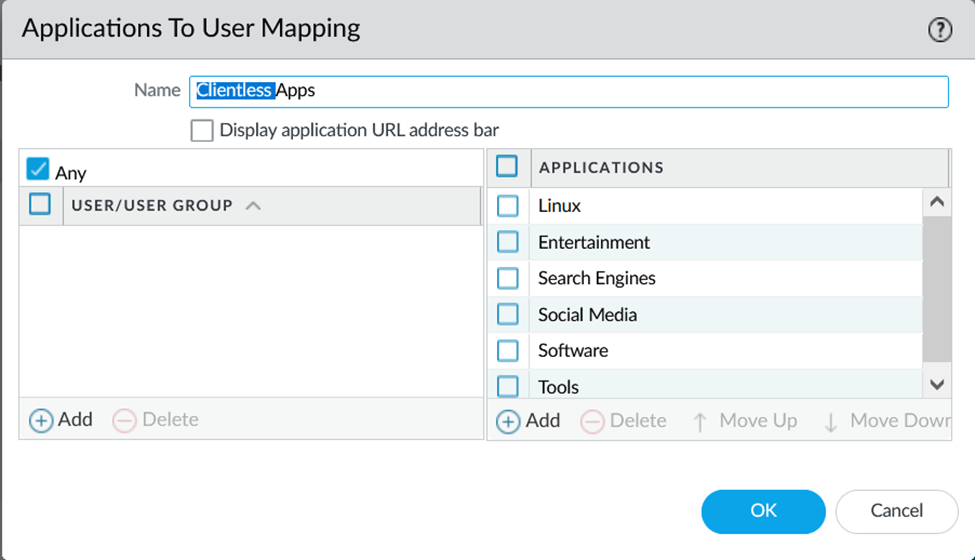
Global Protect would allow connections whenever the user would like to use Global Protect for remote access.



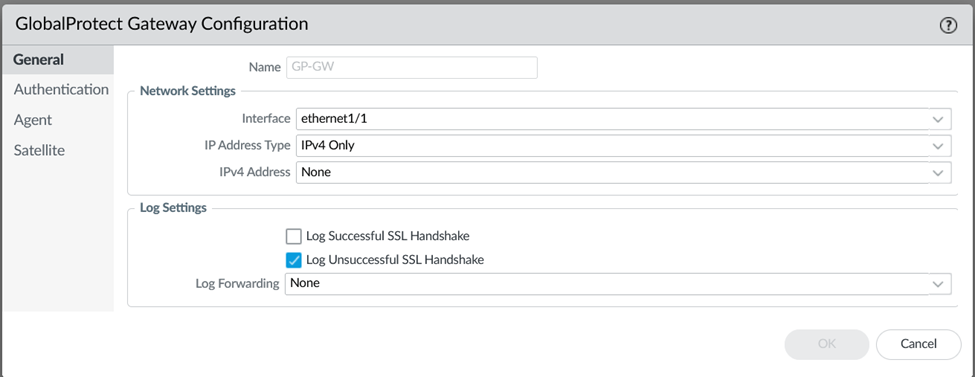
Configuring the portal to allow the user to visit websites without the Global Protect client installed.

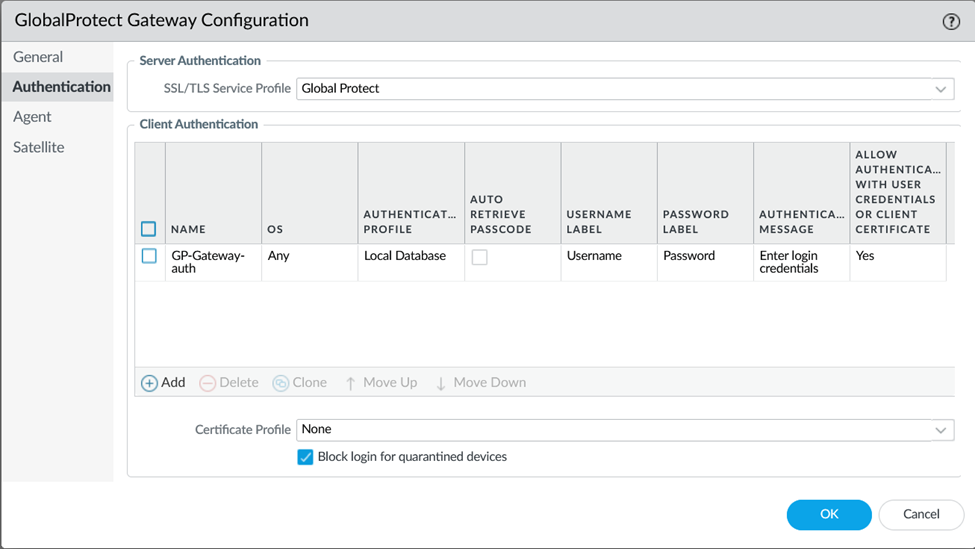


Specifying Apps to appear on the portal when the user logs in through a web browser. In these cases, Clientless App groups are specified, so that you would add apps to the groups without needing to specify every single app in this menu.

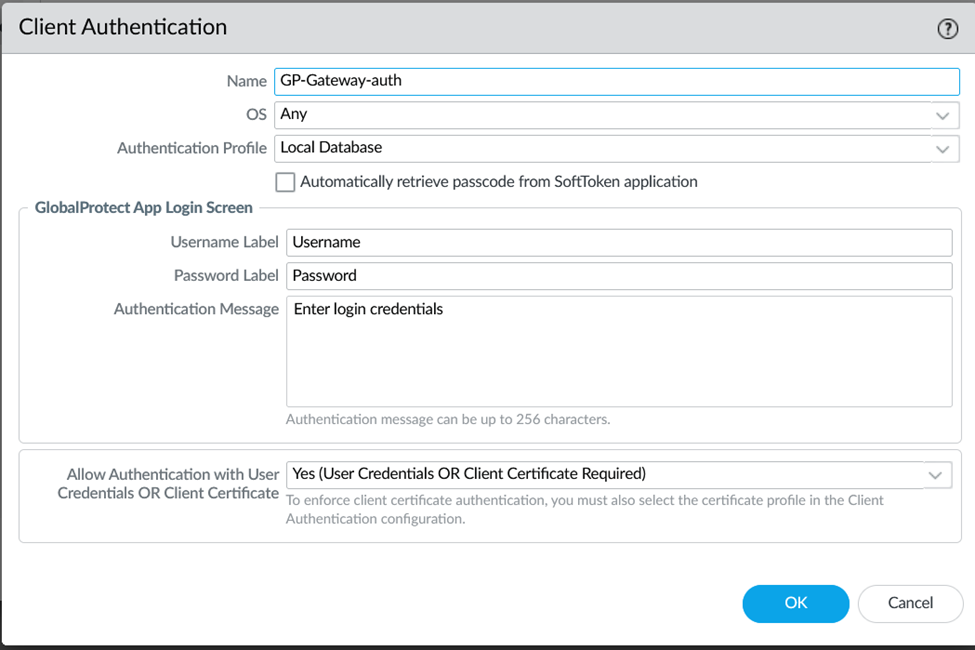


Global Protect Gateway configuration.

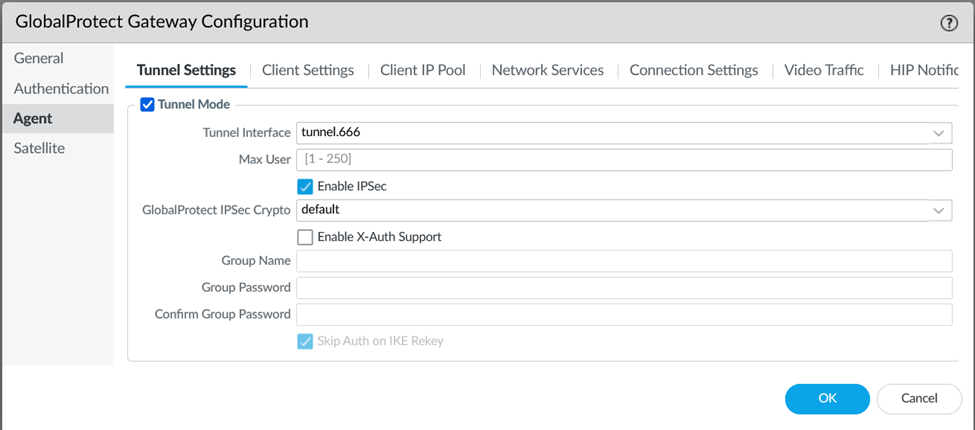




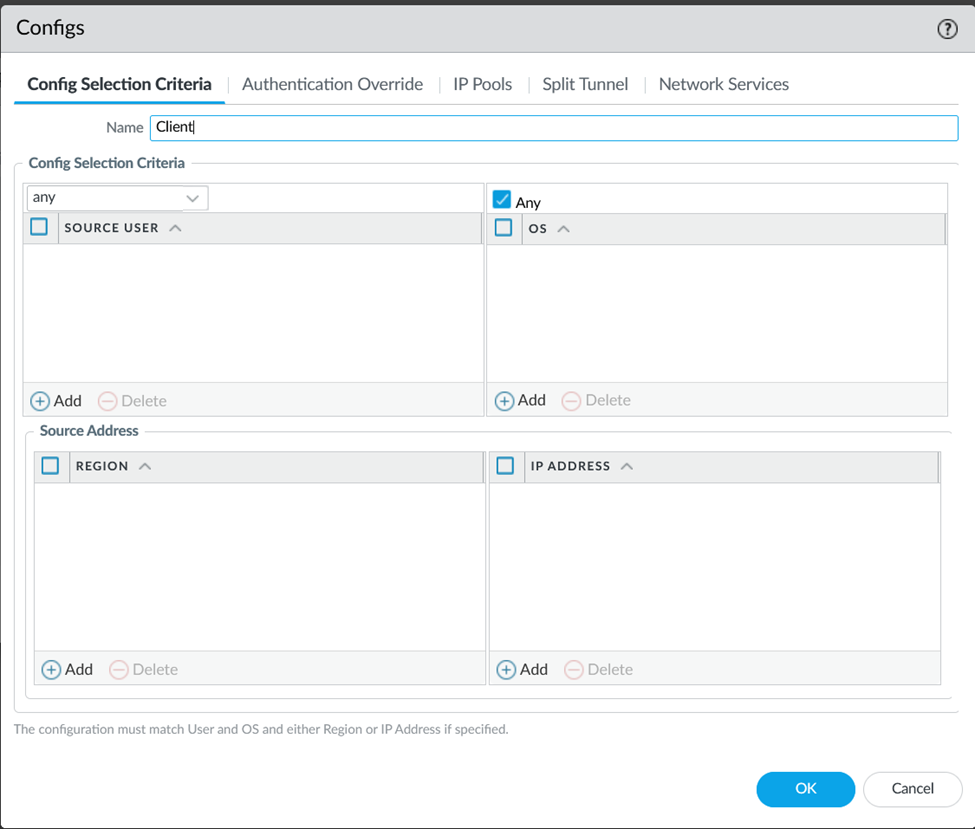
Gateway Authentication configuration



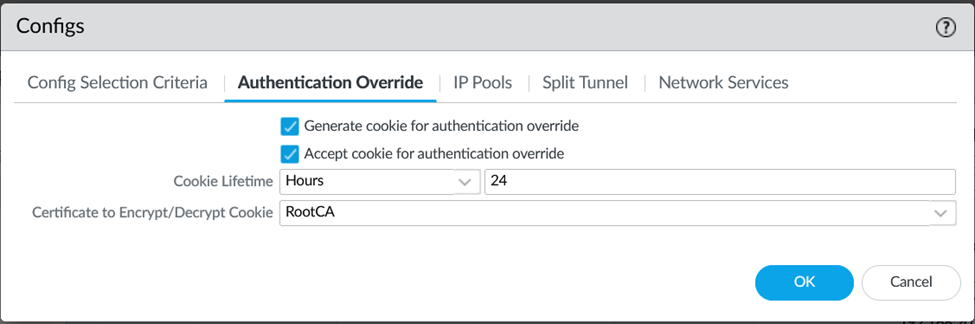
Gateway Agent configuration



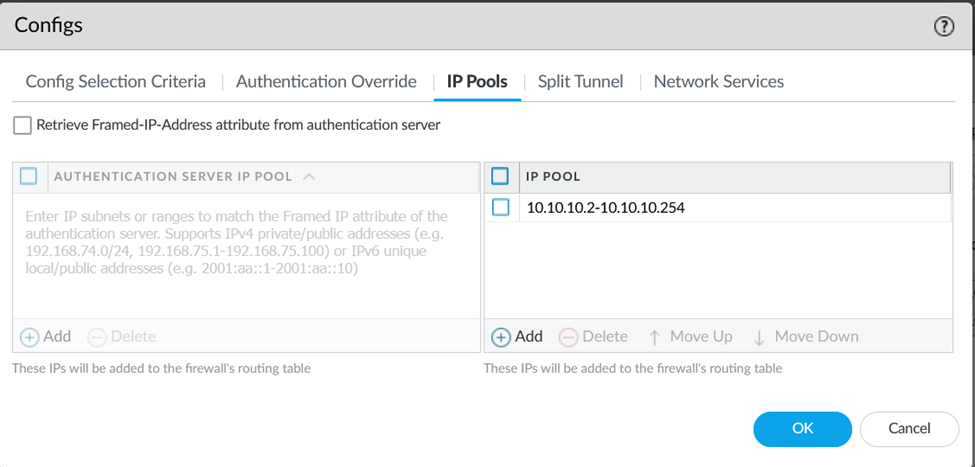
Gateway agent client configuration



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

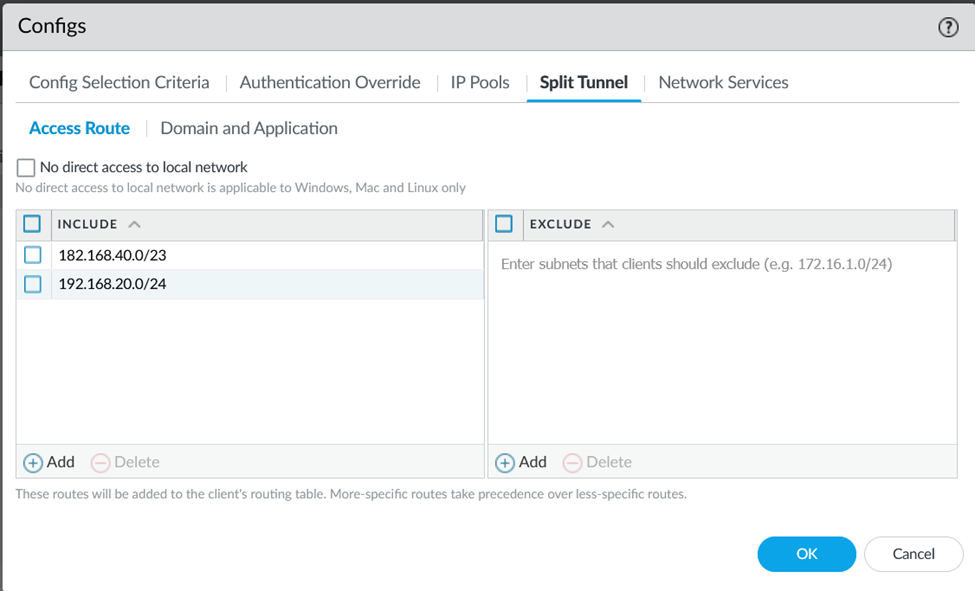


The IP Pool that assigns the clients an ip address that’s available in the address pool.

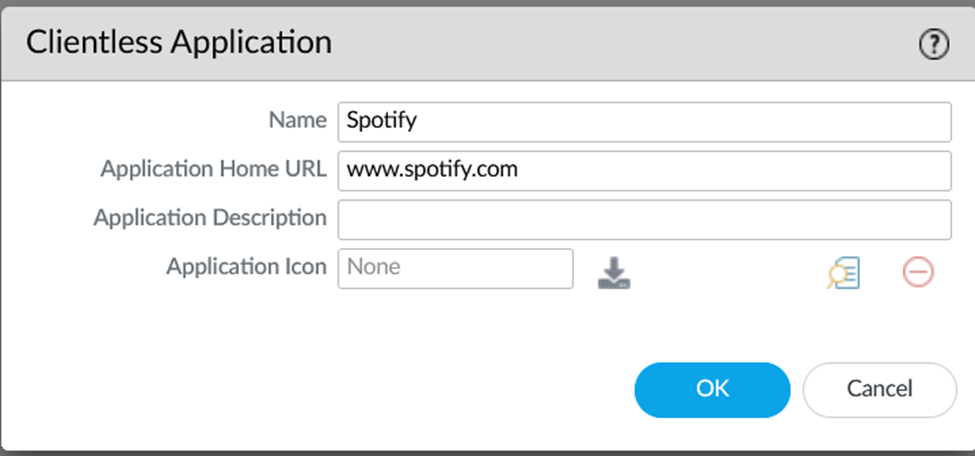


A split tunnel that would give include access to the LAN subnet of the firewall, and the WAN subnet of the internet interface.

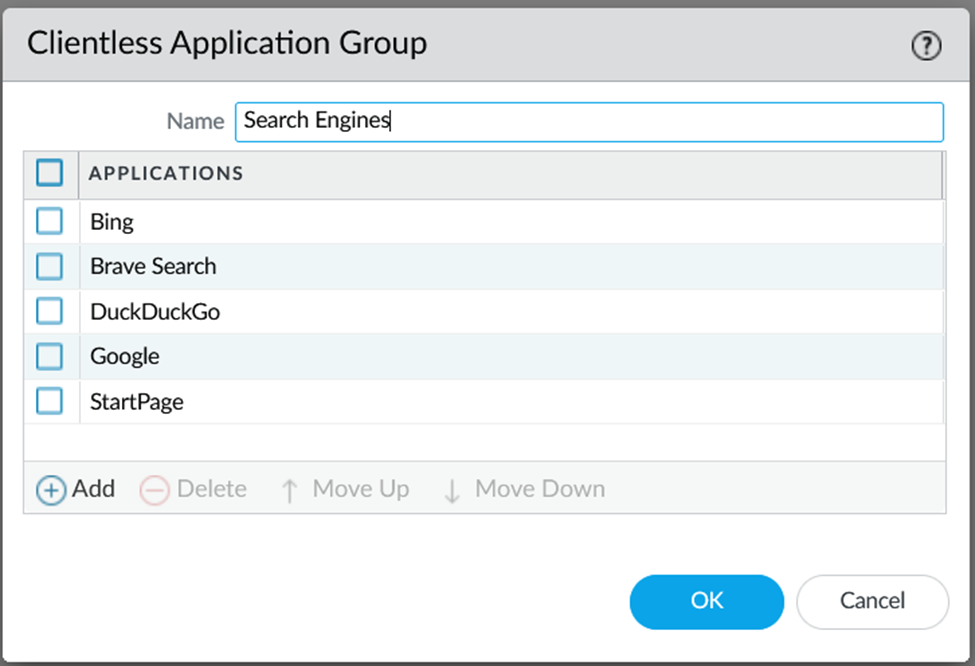
**Fix:** Changed it to “0.0.0.0/0” to have all of the client’s traffic go through the VPN.



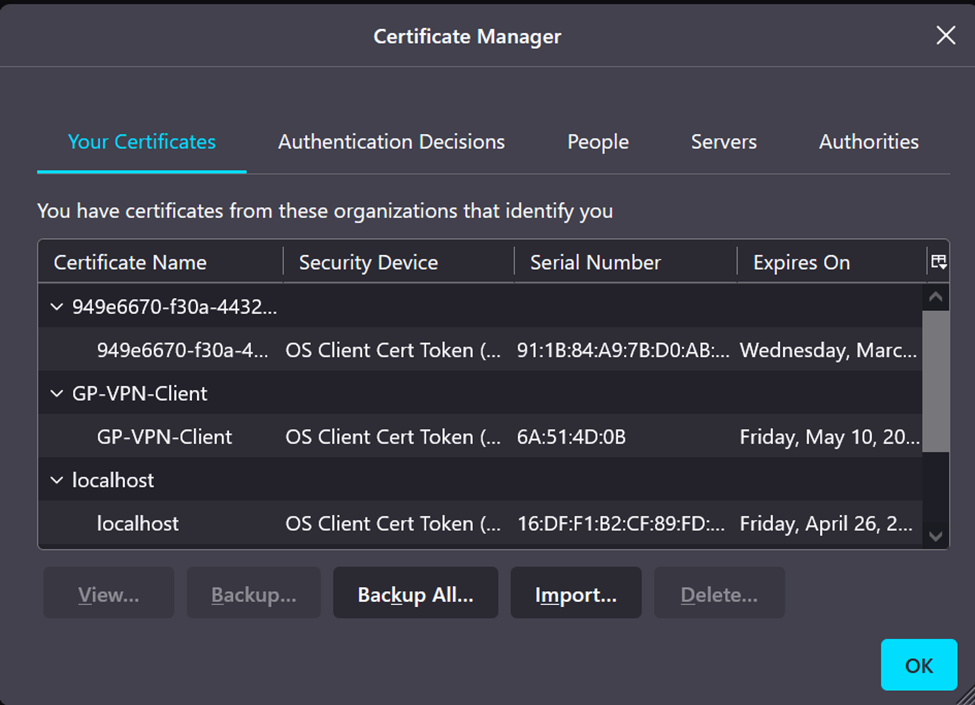
A clientless app that would appear on the portal if the user logged in through a web browser. In this case if the user clicks on this app, it will open Spotify.



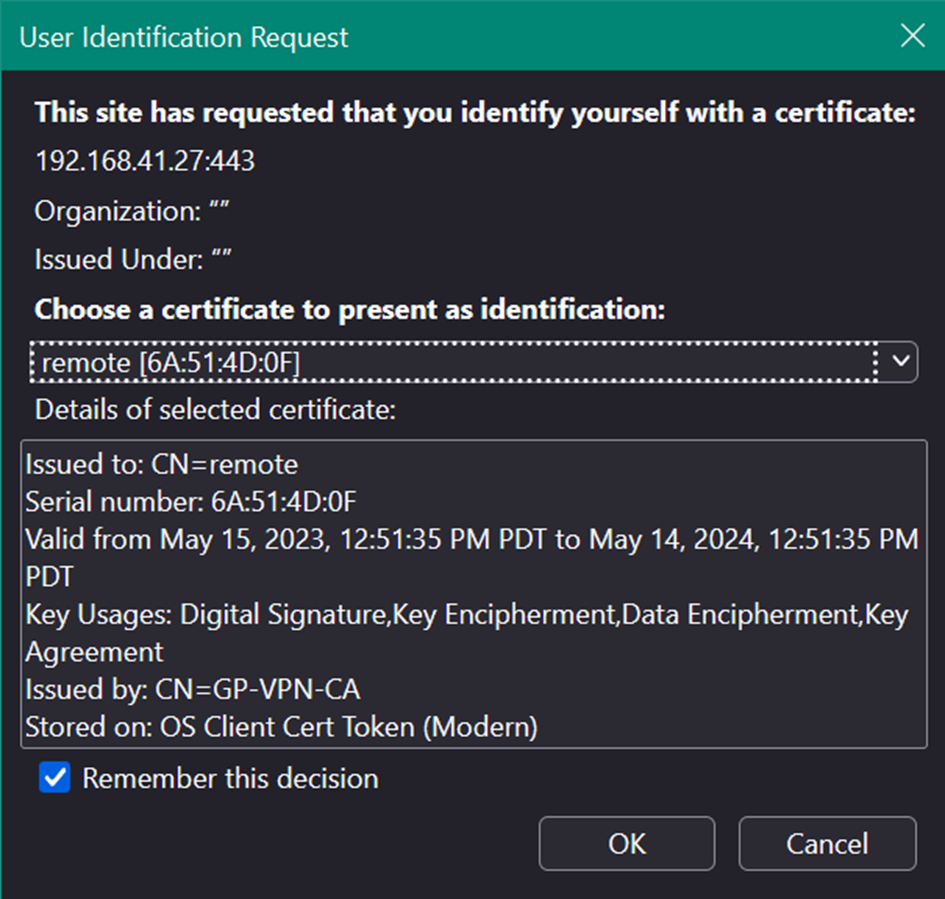
A clientless app group that would contain a group of apps, in this case this group contains search engines. This makes it easier to specify the groups in the clientless configuration rather than specifying every single app. In this case.



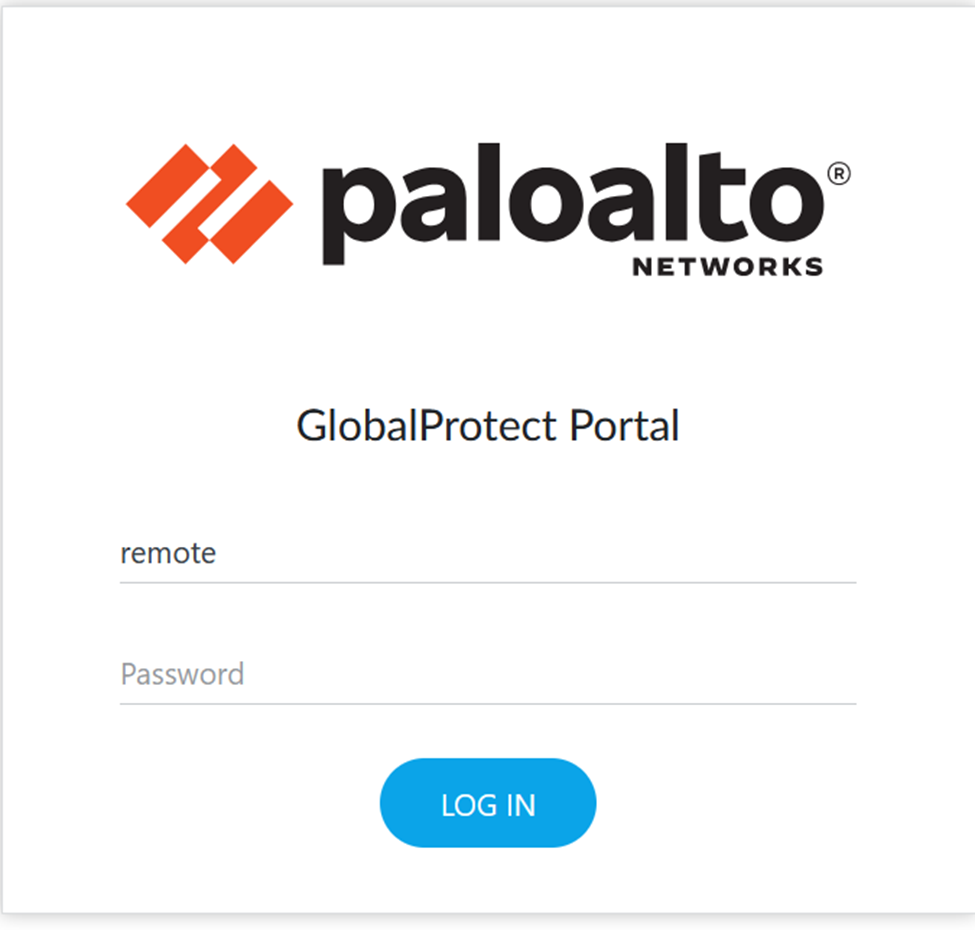
Importing the client certificate into Firefox.



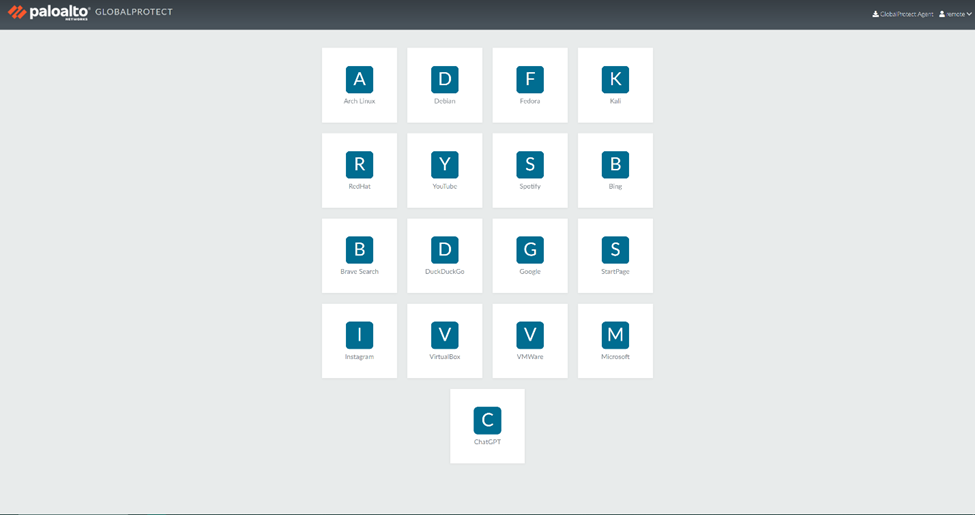
The site asks to specify the certificate for authentication.



The portal prompts the user for a password to login.



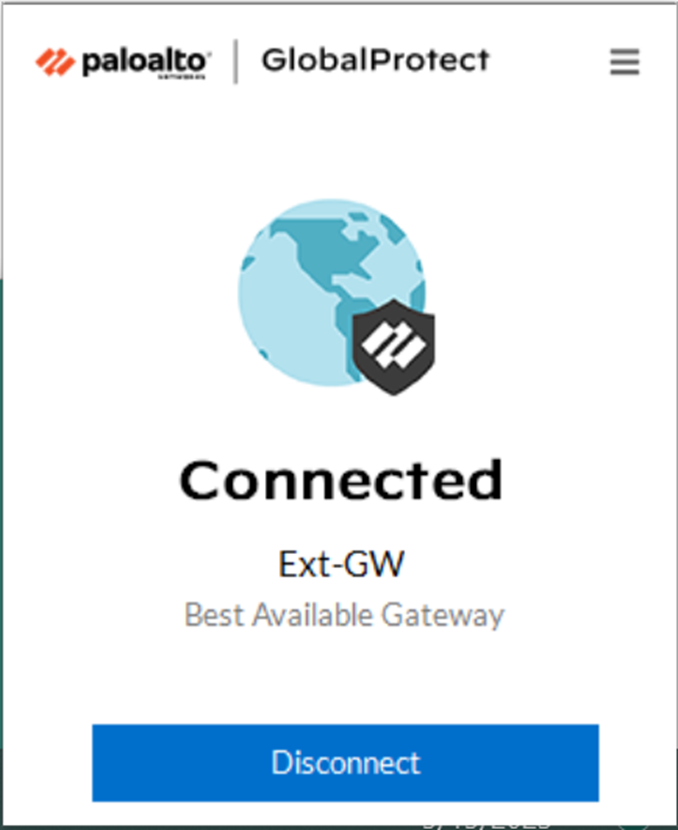
The portal contains clientless apps that the user can visit when they login through a web browser.



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. The last issue we faced was that the clients connected the Global Protect VPN were not able to access the internal management network fixed it by making and adding a NAT policy that any traffic that is meant for the internal network would forward it to the VLAN network. Another issue we had was the Palo Alto client said that it needs a valid certificate, the issue was resolved by exporting the Intermediate certificate onto one device and importing it into “Intermediate Certificates” on the client computer.

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 with Certificates Authentication. 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 with Certificates Authentication. 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.